Gislaine Parra

METODOLOGIA PARA ANÁLISE DE SEGURANÇA APLICADA EM UMA INFRA-ESTRUTURA DE CHAVE PÚBLICA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Olinto José Varela Furtado, Dr.

FLORIANÓPOLIS

2002

Gislaine Parra

METODOLOGIA PARA ANÁLISE DE SEGURANÇA APLICADA EM UMA INFRA-ESTRUTURA DE CHAVE PÚBLICA

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina

Florianópolis, 16 de agosto de 2002.

_____

Prof. Fernando Álvaro Ostuni Gauthier, Dr.
Coordenador

Banca Examinadora

_____

Prof. Olinto José Varela Furtado, Dr.
Orientador

_____

Profª. Elizabeth Specialski, Dra.

_____

Prof. Mauro Faccioni Filho, Dr.

Ofereço esta dissertação a todos os professores, alunos e funcionários do CPGCC.

AGRADECIMENTOS

Aos meus pais, Osvaldo e Geni, pela educação e formação moral, que são a base de todas as minhas conquistas.

Ao Departamento de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, pela qualidade do curso ministrado.

Agradeço ao meu orientador Olinto José Varela Furtado, pela atenção e oportunidade a mim dispensada.

À professora Maria Marta Leite, por toda colaboração e sugestões ao trabalho, mas principalmente pela atenção dispensada à minha pessoa. Deixo registrada a minha admiração pelo carinho com que ela exerce a sua tarefa de educadora.

Aos colegas de mestrado, grandes companheiros durante o período de estudo, que me apoiaram e ajudaram em todos os momentos. Com agradecimentos especiais aos amigos Luciano Ignaczak, Fabiana F. Freund, Luciana Schimt.

Ao professor Fernando Álvaro Ostuni Garthier, coordenador do CPGCC, por todo o esforço demostrado na tentativa de melhoria do curso.

Ao professor Mauro Faccioni Filho, diretor do CTAI, pela colaboração e incentivo a mim dispensados.

Ao CTAI, que possibilitou condições, disponibilizando tempo para o término desta dissertação.

Agradeço a todos que direta ou indiretamente contribuíram para a concretização desta dissertação.

RESUMO

Com o aumento do uso da Internet, cresce o número de informações que se propagam na rede. Automaticamente, a necessidade de proteção dessas informações aumenta em igual proporção. Para atender a essas necessidades, é imprescindível o uso de métodos eficientes, que possam garantir integridade das informações e confiança entre as partes envolvidas. A Infra-estrutura de Chave Pública é um tipo de empresa que utiliza métodos eficientes para oferecer serviços de segurança. Este trabalho descreve conceitos sobre certificados digitais, as técnicas de segurança usadas por estes e os serviços que são garantidos com seu uso. Descreve também os principais componentes necessários para a formação de uma Infra-estrutura de Chave Pública. Faz uma apresentação da norma ISO 17799 e seus controles e apresenta definições sobre Plano de Continuidade de Negócios e suas etapas. A proposta deste trabalho é apresentar uma Metodologia Simplificada para Análise de Segurança, elaborada com base nos controles definidos pela norma ISO 17799. A metodologia poderá ser utilizada por empresas de pequeno porte, porém, a aplicabilidade da metodologia proposta neste trabalho será testada em uma empresa do tipo Infra-estrutura de Chave Pública.

Palavras-chaves: Plano de Continuidade de Negócios, ISO 17799, Infra-estrutura de Chave Pública, Segurança da Informação

ABSTRACT

With the enlargement use of the Internet, the ammount of information that propagate in the network has been growing. Automatically, the necessity of information protection grows in equal proportion. To reach this necessities is indispensable the use of efficient methods that guarante integrity and trustreness of this informations between the parts. ICP is a kind of enterprise that offer such security services. This job describes conceptions about digital certificates, security techniques and services that are safing with security use. Describe either the main components to form na ICP. Make an apresentation of ISO 17799 standard and his controls and introduce definitions about PCN and his stages. The proposal of this work is to present a Simplified Methodology for Analysis of Security, based on the controls defined for ISO 17799 standard. The methodology can be used by small business companies, however, the applicability of the methology ptoposed in thes work will be tested in a Infrastructure of Public Key´s company.

Key words: Business Continuity Plan, ISO 17799, Infrastructure of Public Key´s, Security of Informations

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SIGLAS

AC	Autoridade Certificadora
AC-Raiz	Autoridade Certificados Raiz
BIA	Business Impact Analisys
DRI	Disaster Recovery Institute International
ICP	Infra-estrutura de Chave Pública
ISO	International Organization for Standardization
OIC	Office of the Information Commissioner of Canada
ITU	International Telecommunication Union
LCR	Lista de Certificados Revogados
M.A.S	Metodologia para Análise de Segurança
PC	Plano de Contingência
PCN	Plano de Continuidade de Negócios
RCMP	Royal Canadian Mounted Police
TI	Tecnologia da Informação

CAPÍTULO I
INTRODUÇÃO

1.1 Considerações Iniciais

O avanço tecnológico tornou a Internet cada vez mais popularizada, transformando-se em uma ferramenta essencial para as empresas e para o público em geral. O número de transações feitas na Internet e o número de pessoas comprando pela rede aumenta a cada dia.

Com a comercialização e o compartilhamento das informações através da Internet, as empresas estão revendo seus antigos conceitos e buscando mecanismos de segurança, com o objetivo de proteger os bens considerados mais valiosos, dentre eles a informação.

A informação é um bem importante e vital em uma organização. Como qualquer outro bem do negócio, tendo valor financeiro ou não, precisa ser protegida. Esta proteção é necessária para resguardar os interesses da organização diante do grande número de ameaças, assegurando a continuidade de seus negócios.

A segurança é um dos aspectos fundamentais para a sobrevivência de uma empresa. Uma das principais preocupações de um cliente, ao procurar um serviço em que ele deva disponibilizar seus dados pessoais na rede, é a segurança desses dados.

A manutenção da confidencialidade, da integridade e da disponibilidade das informações são necessidades essenciais para manter uma organização competitiva e para proteger sua imagem e reputação diante de outras empresas e de seus clientes. Por esse motivo o tema “Segurança” passou a ser imprescindível nas reuniões estratégicas dos executivos (MAIA, 2001).

A Segurança da Informação pode ser compreendida por três aspectos principais: segurança lógica, segurança física e segurança técnica. Todos esses aspectos são importantes dentro de uma organização e devem ser protegidos na mesma proporção. O investimento

desproporcional em um dos aspectos pode ocasionar perdas de todos os outros recursos, em virtude de uma falha nos sistemas mais vulneráveis.

A ISO 17799 apresenta uma extensa lista de controles de proteção das informações em uma abordagem integrada, combinando segurança física, lógica e técnica. A norma é uma ferramenta poderosa que auxilia na identificação de vulnerabilidades e apresenta mecanismos para minimizar danos e proporcionar a continuidade nos negócios.

Existem várias empresas que fornecem serviços de segurança. Entre elas estão as Autoridades Certificadoras - ACs, que cada vez mais se tornam imprescindíveis, pois em se tratando de Internet, o termo segurança é a alma do negócio. As ACs emitem certificados digitais, que têm a função de tornar as compras pela Internet mais seguras, comprovar a idoneidade de empresas, entre outras garantias.

Para poder garantir a segurança de outras empresas, é necessário que as ACs tenham um alto nível de responsabilidade. A segurança de suas informações e a continuidade de seus negócios são aspectos que devem ser garantidos para que a segurança fornecida pelas ACs seja eficiente.

Portanto, tão importante quanto a segurança da informação é a continuidade dos negócios. A empresa deve estar segura de que, se incidentes acontecerem, ela esteja preparada para a retomada do negócio em tempo hábil, de forma a não prejudicar seus interesses.

A preparação das empresas para enfrentar episódios inesperados é elaborada em um planejamento chamado Plano de Continuidade de Negócios. Esses planos são realizados por consultores de segurança, que preparam as empresas com medidas de contingência, considerando o tempo, a cultura nelas preservada e a rapidez do crescimento da perda à medida que o tempo passa.

Um Plano de Continuidade de Negócios deve ser elaborado a partir do princípio de que um nível aceitável de segurança já tenha sido atingido pela organização e de que a conscientização da importância da segurança já seja um fato concreto para os envolvidos no negócio.

Este trabalho apresenta uma metodologia de análise de segurança básica e concisa, para fornecer às empresas de pequeno porte, mais especificamente para ACs, uma ferramenta para avaliação de requisitos mínimos de segurança para a garantia da continuidade de seu negócio.

1.2 Hipótese

Com o grande número de informações que se encontram disponíveis na rede mundial, e a intensidade das transações realizadas através dela, as empresas estão enfrentando uma concorrência sem fronteiras. Algumas estão oferecendo um diferencial: a segurança da informação. Para isso, as empresas adotaram o uso de documentos eletrônicos, assinados digitalmente, que permitem garantir a autenticidade e a integridade das transações feitas pela Internet. Para que os documentos sejam assinados digitalmente, é necessário que uma empresa forneça este serviço. O tipo de empresa que fornece este serviço é denominada de Infra-Estrutura de Chave Pública.

Com o avanço tecnológico e a aprovação da tramitação de documentos assinados digitalmente, o governo brasileiro sentiu a necessidade de implantar uma ICP brasileira (ICP-Brasil). Isso torna possível a assinatura de documentos digitais brasileiros e sua validade jurídica, não precisando mais ser efetuada por órgão do exterior.

Em razão da seriedade e do grau de importância depositados na ICP-Brasil, acredita-se que a continuidade de seus negócios, garantindo a continuidade do atendimento a seus clientes, é um aspecto de extrema importância. Por este motivo, órgãos que executam serviços de grande responsabilidade devem elaborar e manter atualizado um Plano de Continuidade de Negócios. Isto é necessário para evitar que, em caso de problemas no futuro, aconteça a paralisação dos processos, o que conseqüentemente poderia afetar a qualidade de seus serviços. A utilização do Plano de Continuidade de Negócios (PCN) por este tipo de empresa proporciona uma segurança essencial para seus clientes.

Conforme já mencionado, a implantação de um PCN deverá ser feita a partir de um nível aceitável de segurança. Sendo assim, o primeiro passo da organização deve ser alcançar este nível aceitável. A partir daí, ela poderá buscar empresas que forneçam serviços de segurança, preparando-a para enfrentar problemas futuros.

1.3 Objetivos

1.3.1 Objetivo Geral

- Propor uma metodologia simplificada, para auxiliar empresas que emitem certificados digitais a analisar a situação atual de segurança.

1.3.2 Objetivos Específicos

- apresentar definições de Certificados Digitais e sua composição;
- estudar técnicas de Criptografia, Função Hash, Assinatura Digital;
- apresentar a estrutura dos Certificados Digitais;
- apresentar definições de ICP e descrição dos seus principais componentes;
- estudar a norma ISO 17799;
- analisar os modelos de Plano de Continuidade de Negócios e apresentar um modelo existente;
- propor uma metodologia para análise de segurança;
- testar a metodologia em uma ICP e apresentar os resultados da análise.

1.4 Descrição dos Capítulos

Este trabalho esta estruturado em quatro capítulos principais:

Capítulo I – apresenta de forma sucinta o escopo do trabalho contendo a hipótese, objetivos e sua estrutura.

Capítulo II – é apresentada a Revisão de Literatura, através da qual pretende-se caracterizar o estudo.

Capítulo III - apresenta uma metodologia simplificada, elaborada com base em um modelo proposto por Saldanha (2000) em seu livro Introdução a Planos de Continuidade e Contingência Operacional e nos requisitos da norma ISO 17799, que poderá ser utilizada pelas ICPs e por empresas de pequeno porte para a análise da situação da segurança

do momento. Apresenta, ainda, o resultado da aplicação da metodologia, testada em uma Infra-estrutura de Chave Pública, além de gráficos que permitem uma visão clara da situação de segurança da empresa em questão.

Capítulo IV - apresenta as considerações finais e sugestões para trabalhos futuros. A seguir, é apresentado as Referências Bibliográficas e os Anexos.

CAPÍTULO II
REVISÃO DE LITERATURA

Neste capítulo, visando uma melhor compreensão do tema em questão procurar-se-á, de maneira sucinta, definir Certificados Digitais e o conjunto de campos padrão que os compõem; Infra-estrutura de Chave Pública – ICP; a ISO 17799 e Plano de Continuidade de Negócios.

2.1 Certificados Digitais

Os Certificados Digitais fazem o papel de uma carteira de motorista, passaporte ou alvará eletrônico para transações em meio digital. A apresentação de um Certificado Digital é feita de forma eletrônica para comprovar a identidade ou a autorização de acesso a informações ou a serviços. Segundo Feghhi e Willians (1999), Certificado Digital é uma associação entre uma chave pública e uma entidade. Os Certificados Digitais garantem a idoneidade dos dois lados de uma transação. De um lado, certifica a existência e autenticidade do cliente; e do outro, certifica que este cliente estará fazendo negócio com uma empresa verdadeira.

Para definir Certificados Digitais e o conjunto de campos padrão que os compõem, toma-se por base uma Infra-estrutura de Chaves Públicas que utiliza certificados definidos pela recomendação X.509 do *International Telecommunication Union – Telecommunication Standardization Sector* (ITU-T). A recomendação X.509 define o formato dos Certificados Digitais e suas funcionalidades. São apresentados também os conceitos de Criptografia, Autenticação, Função Resumo e Assinaturas Digitais.

Certificados Digitais são usados para ligar uma entidade a uma chave pública (ADAMS e LLOYD 1999). Desta maneira é possível identificar uma pessoa ou dispositivo através de um Certificado Digital.

No mecanismo tradicional de identificação, a carteira de identidade garante que alguém que se diz ser "Alice" é realmente a "Alice". Isto é possível porque existe um órgão, a Secretaria de Segurança Pública, que, através da certidão de nascimento e foto da pessoa, emite a carteira de identidade. No mundo digital, algo similar acontece. Alice deve ir a uma Autoridade Certificadora, com seus documentos de identificação tradicionais (CPF, carteira de identidade), e lá obter seu Certificado Digital.

2.1.1 Técnicas de Segurança Fornecidas pelos Certificados Digitais

Para um melhor entendimento sobre os componentes e o funcionamento dos Certificados Digitais, serão abordados alguns conceitos importantes de Criptografia, Autenticação, Função Resumo e Assinaturas Digitais, que são técnicas de segurança fornecidas pelos Certificados Digitais.

- **Criptografia**

Segundo Garfinkel e Spafford (1999), criptografia é um conjunto de técnicas usadas para transformar textos legíveis em textos cifrados, de forma que somente pessoas autorizadas tenham acesso a essas informações. A criptografia faz uso de uma combinação entre uma função complexa, ou seja, um algoritmo criptográfico, e uma chave para realizar a transformação dos dados. Após a codificação dos dados, a criptografia impede o processo inverso, ou seja, não é possível obter a reprodução de textos originais a partir de textos cifrados sem a posse da chave que foi utilizada para cifrá-lo. Além disso, a criptografia dificulta qualquer tentativa de se descobrir a chave que pode fazer essa decodificação. Conforme Stinson (1995), o principal objetivo da criptografia é permitir a comunicação segura entre duas partes, realizada através de um canal não seguro, de tal forma que uma terceira pessoa ou entidade não consiga entender o conteúdo que está sendo transmitido.

A criptografia busca garantir os seguintes serviços:

- **Autenticação:** Identifica um indivíduo ou dispositivo em uma rede, garantindo que este é quem diz ser.
- **Integridade:** Serviço que assegura que um documento não foi alterado a partir de um determinado momento.
- **Confidencialidade:** Busca garantir o segredo de uma mensagem, ou seja, ninguém que não possua autorização acessará o conteúdo de uma mensagem.

A criptografia é uma técnica milenar, que foi usada pelo generais gregos para enviar mensagens em código aos comandantes de campo. As técnicas usadas antigamente eram baseadas em substituição e transposição. Na técnica de substituição, as letras de um texto original eram substituídas por outras letras. Na técnica de transposição, as mensagens eram escritas em tabelas e lidas coluna por coluna (GARFINKEL e SPAFFORD, 1999). Recentemente, a criptografia tornou-se uma ferramenta utilizada nos negócios, principalmente no comércio eletrônico, e utiliza técnicas mais aprimoradas. Existem dois tipos de criptografia em uso hoje: criptografia simétrica e criptografia assimétrica.

- Criptografia Simétrica

A criptografia simétrica consiste no uso de um algoritmo e uma chave (STALLINGS, 1999). Sua principal característica é utilizar somente uma chave para autenticar, garantir a integridade e a confidencialidade de uma mensagem.

A chave é gerada pelo emissor da mensagem e usada para cifrar o texto que se deseja transmitir para uma ou mais pessoas. A criptografia simétrica necessita que todos os indivíduos envolvidos no processo tenham conhecimento da chave, pois a mesma chave usada para criptografar a mensagem será usada para decriptografar. Um grande problema deste modelo é garantir o compartilhamento do segredo de forma confiável. Outro problema surge se o segredo for compartilhado entre mais de duas pessoas: a autenticação não pode mais ser assegurada. Isso porque qualquer um poderá cifrar uma mensagem usando a chave de conhecimento do grupo, alegando ser outra pessoa que possua conhecimento da mesma chave (STALLINGS, 1999).

A Figura 1 apresenta o funcionamento da criptografia simétrica. Nela A representa o emissor junto à mensagem com o texto original. Esta é criptografada, gerando uma mensagem cifrada, que é enviada pela rede. Ao chegar no receptor, representado por B, a

mensagem é decifrada usando a mesma chave usada para criptografar, obtendo-se assim o texto original.

Figura 1 - Funcionamento da criptografia simétrica

- Criptografia Assimétrica

De acordo com Stallings (1999), a criptografia assimétrica ou de chave pública utiliza duas chaves diferentes, matematicamente relacionadas, sendo uma privada e outra pública. Um texto cifrado com a chave pública do receptor da mensagem somente poderá ser decifrado com a chave privada de quem recebe.

A garantia da confiança está no fato de que cada usuário deverá gerar seu par de chaves. A chave privada deve ser mantida em segredo e não poderá ser utilizada por ninguém, exceto pela pessoa a qual ela pertence. A chave pública, ao contrário, deve ser disponibilizada para ser utilizada por qualquer aplicação ou indivíduo.

A Figura 2 apresenta o funcionamento da criptografia assimétrica. Na figura, A (emissor) detém a mensagem com o texto original. Esta é criptografada utilizando-se a chave pública de B (receptor). Gera-se uma mensagem cifrada, que é enviada pela rede. Ao chegar em B, a mensagem é decifrada usando chave privada de B, obtendo-se assim o texto original.

Figura 2 - Funcionamento da criptografia assimétrica

- **Autenticação**

A autenticação provê a garantia de que as entidades envolvidas em uma transação são quem elas dizem ser. Existem dois tipos de autenticação. O primeiro possibilita a autenticação de uma entidade durante uma conexão ativa. O exemplo deste tipo é um site que forneça garantias de sua identidade. O outro tipo é a autenticação de mensagens que dê a certeza de que seu conteúdo está íntegro e que se originou de uma determinada entidade. Uma autenticação pode ser feita dos seguintes modos (FEGHHI e WILLIANS, 1999):

- Algo que você sabe: A autenticação é feita por meio de algum conhecimento específico do indivíduo. Este conhecimento pode ser uma senha ou um número de identificação pessoal.

- Algo que você tem: A entidade é identificada pela posse de algo. O objeto pode ser, por exemplo, um disquete ou um *smart card* com a chave privada armazenada.

- Algo que você é: A entidade utiliza alguma medida biométrica para identificação. Por exemplo, a impressão digital ou a íris.

A autenticação também pode ser feita por meio da combinação de duas ou mais formas citadas. Por exemplo, o indivíduo pode ter a necessidade de digitar uma senha, além de ter sua impressão digital verificada.

- **Função Resumo ou Hash**

A Função Resumo ou Hash produz uma "impressão digital" de um arquivo, mensagem ou bloco de dados. A Função Resumo recebe como entrada mensagens de tamanhos variados e sempre produz um resultado de tamanho fixo como saída. O tamanho da saída pode variar de acordo com o algoritmo usado (STALLINGS, 1999).

Funções Resumo são consideradas funções de caminho único, ou seja, o conteúdo de uma mensagem não pode ser determinado através de seu resultado. Outra característica deste tipo de função é que seu resultado deve ser totalmente alterado se apenas um *bit* de uma mensagem é mudado.

Através da "impressão digital" resultante de uma Função Resumo a integridade dos dados pode ser assegurada, pois é computacionalmente impossível criar uma Função Resumo de uma mensagem levando em consideração um resultado já existente (STALLINGS,1999).

Função Resumo é denominada também como: *Message Digest,* Função de Condensação ou *Hash*.

- **Assinatura Digital**

A Assinatura Digital utiliza a Função *Hash*, apresentada anteriormente, para garantir a autenticidade e a integridade de dados. Para criar a Assinatura Digital de uma mensagem, o usuário pode utilizar uma chave privada específica para assinatura ou a chave privada do par de chaves usado para garantir a confidencialidade dos dados (ADAMS e LLOYD, 1999).

Para gerar uma Assinatura Digital, primeiro é criado um resumo da mensagem. Após sua criação, o resumo é cifrado utilizando-se a chave privada do emissor. O resultado é a Assinatura Digital da mensagem.

No momento em que o usuário recebe a mensagem, ele cria um novo resumo da mensagem recebida. Em seguida, ele decifra o resumo recebido junto com a mensagem, utilizando a chave pública do emissor. Se o resumo criado pelo receptor for idêntico ao resumo recebido, é possível garantir a integridade da mensagem e assegurar que os dados foram assinados pela chave privada correspondente àquela chave pública (STALLINGS, 1999).

A Figura 3 apresenta a geração de uma mensagem utilizando Assinatura Digital.

Figura 3 - Geração de uma mensagem com Assinatura Digital

O emissor A possui a mensagem com o texto original. Ele aplica a Função Resumo, acrescenta o resultado da função na mensagem, criptografa usando sua chave privada e envia este pacote pela rede.

A Figura 4 apresenta a maneira em que é feita a verificação de uma mensagem com Assinatura Digital.

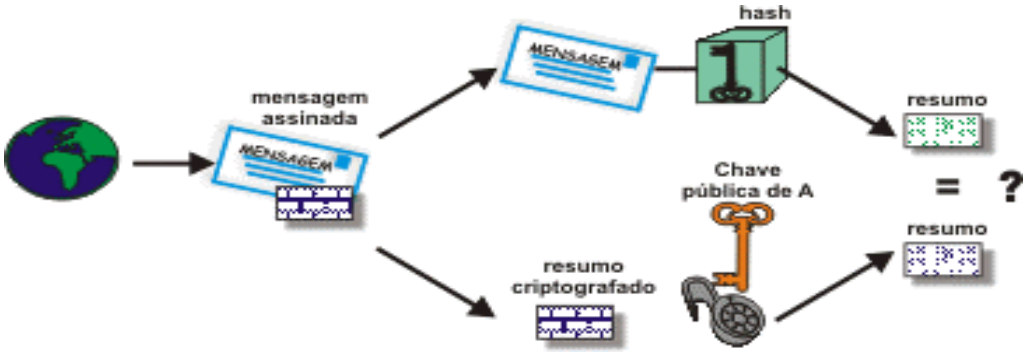
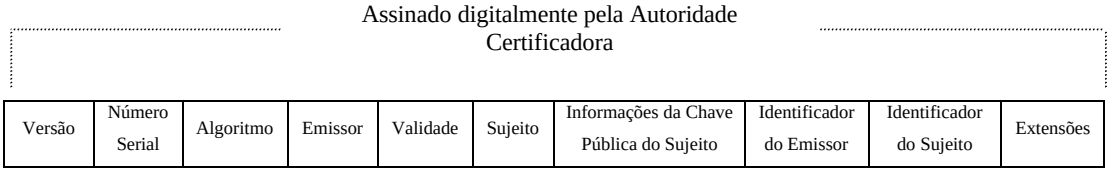


Figura 4 - Verificação de uma mensagem com Assinatura Digital

Ao receber a mensagem, o receptor B obtém o texto original e o resumo da mensagem criptografado. B decifra o resumo utilizando a chave pública de A. Em seguida, B cria um novo resumo da mensagem que recebeu, utilizando a chave pública de A. Com o resultado deste resumo, B faz uma comparação com o resumo recebido.

2.1.2 Estrutura dos Certificados Digitais

Embora existam vários tipos de certificados em uso na Internet, a maior aceitação é pela recomendação X.509 da ITU-T. Um Certificado Digital é formado por um conjunto de campos definidos pela recomendação X.509 versão 3, os quais são mostrados na Figura 5 (ADAMS e LLOYD, 1999).



Fonte: ADAMS e LLOYD (1999).

Figura 5 - Conjunto de campos que constitui a formação de um Certificado Digital.

De acordo com as recomendações X.509, as definições dos campos dos Certificados Digitais são:

- **Versão:** Identificador da versão do certificado.
- **Número Serial:** Identificador único de um certificado em relação à Autoridade Certificadora que o emitiu.
- **Identificador do Algoritmo de Assinatura:** Campo que identifica o algoritmo usado pela Autoridade Certificadora para assinar o certificado.
- **Nome do Emissor:** Informações que identificam a Autoridade Certificadora emissora do certificado.
- **Período de Validade:** Intervalo de tempo em que um certificado pode ser considerado válido. Este campo possui a data em que o certificado foi emitido pela Autoridade Certificadora e a data de expiração do certificado.
- **Sujeito:** Dados de identificação do indivíduo ou dispositivo para o qual o certificado foi emitido.
- **Informações sobre a Chave Pública do Sujeito:** Apresenta a chave pública do certificado juntamente com o identificador do algoritmo que ela deve utilizar em suas operações.
- **Identificador do Emissor:** Valor único para a identificação do emissor do certificado.
- **Identificador do Sujeito:** Valor usado para a identificação do possuidor do certificado.

- **Extensões:** A versão 3 da recomendação X.509 definiu a utilização de campos de extensão com a finalidade de tornar mais flexível a utilização dos Certificados Digitais (UNION, 1997).

Um Certificado Digital é constituído de três partes. A primeira parte é o conjunto de campos padrão que seguem a recomendação X.509. A segunda parte contém as extensões, que são campos que podem variar de acordo com o tipo do certificado. A última parte é a Assinatura Digital do certificado efetuada pela Autoridade Certificadora que o emitiu (ADAMS e LLOYD,1999).

Um Certificado Digital é sempre assinado por uma Autoridade Certificadora. Esta é responsável pela validação de determinados dados que são incluídos no certificado.

2.1.3 Tipos de Certificados Digitais

Atualmente o Certificado Digital é base para a utilização da *web* de forma segura. Empresas que vendem produtos pela Internet, bancos e outras entidades que necessitam de segurança, precisam adquirir um Certificado Digital de uma Autoridade Certificadora para prover acesso seguro. Este exemplo é apenas um dos possíveis usos de Certificados Digitais: garantia de comunicação segura a um site específico. Os certificados podem ser emitidos para outros fins, conforme descrição feita a seguir:

- **Certificados de AC (Autoridade Certificadora)**: são utilizados para emitir outros certificados. São auto-assinados ou assinados por uma AC de nível superior.
- **Certificados de servidor**: são utilizados para identificar um servidor.
- **Certificados pessoais**: são utilizados para a autenticação do cliente.

A garantia dos dados desses certificados são de responsabilidade da Autoridade Certificadora que o emitiu. Esta também é responsável por manter e divulgar uma Lista de Certificados Revogados (LCR, ver tópico a seguir). Os certificados que estiverem nesta lista podem ter sido roubados, perdidos ou simplesmente estar sem utilidade ou fora do prazo de validade (ADAMS e LLOYD, 1999).

2.1.4 Lista de Certificados Revogados – LCR

Lista de Certificados Revogados – LCR, é uma estrutura de dados assinada digitalmente pela Autoridade Certificadora que a emitiu. A LCR contém uma lista de certificados que não devem ser considerados válidos.

Embora um Certificado Digital possua uma data para sua expiração, algumas vezes é necessário que sua validade seja negada antes do término deste prazo. Assim, um certificado pode ser revogado e, a partir deste momento, ele constará em uma lista contendo um conjunto de certificados inválidos. Uma revogação pode ser efetuada por um dos seguintes motivos:

- **Comprometimento da Chave Privada do Certificado:** Indica que a chave privada do sujeito pode estar comprometida, tornando o certificado do sujeito não confiável.
- **Comprometimento da Chave Privada da Autoridade Certificadora:** A chave privada da Autoridade Certificadora que emitiu o certificado pode estar comprometida. Com isso, não se deve mais confiar nos certificados emitidos por ela.
- **Mudança de Filiação:** Algumas das informações do sujeito contidas no certificado foram alteradas. Assim, um novo certificado deve ser emitido.
- **Atualização:** Indica que o certificado foi atualizado.
- **Cancelamento da Operação:** O certificado não será mais utilizado para o propósito ao qual ele foi emitido.
- **Suspensão Temporária**: Indica que o certificado está temporariamente incluído na LCR. Atribuindo esta suspensão ao certificado, ele poderá ser retirado da LCR após um período de tempo ou revogado definitivamente.
- **Não Específico**: O certificado consta na LCR por algum motivo diferente dos apresentados anteriormente (HOUSLEY e POLK, 1999).

2.2 Infra-Estrutura de Chave Pública - ICP

Uma Infra-estrutura de Chaves Públicas (ICP) é um conjunto de serviços de segurança capaz de proporcionar o uso e gerenciamento da criptografia de chave pública, assim como os certificados digitais, incluindo o gerenciamento de chaves e sua política de

uso. Uma ICP é formada por um conjunto de componentes. Cada componente executa uma função específica.

Uma Infra-estrutura de Chave Pública é organizada de diferentes maneiras, dependendo de seus objetivos. Para isso são usadas hierarquias, em que cada uma decide em quem cada entidade deve ou não confiar. A hierarquia isolada é a mais utilizada atualmente (ADAMS e LLOYD, 1999). Este tipo de hierarquia será conceituado no item 2.2.2.

O objetivo de uma Infra-estrutura de Chave Pública é possibilitar que indivíduos consigam obter um certificado digital e garantir a autenticidade dos dados contidos nele.

2.2.1 Componentes

Componentes são formados por procedimentos que possibilitam constituir uma Infra-estrutura de Chave Pública. Para que uma Infra-estrutura de Chave Pública execute todas as funções, estas são atribuídas aos seus devidos componentes.

Alguns dos principais componentes de uma ICP são:

- Autoridade Certificadora (AC).
- Autoridade de Registro.
- Módulo Público.
- Diretório Público.

- **Autoridade Certificadora (AC)**

Autoridades Certificadoras são entidades responsáveis pela assinatura, emissão de certificados digitais e controle dos certificados revogados. Em razão de sua incumbência, devem ser entidades nas quais todos os indivíduos que farão parte da comunicação depositem sua confiança.

Na prática, o papel da AC é exercido da seguinte forma: o navegador que está sendo utilizado tem uma lista das ACs confiáveis. Assim, ao ser apresentado a um certificado digital durante uma comunicação, o navegador faz uma busca e uma comparação, verificando se a AC do certificado consta na lista. Se for constatada a existência da AC na lista, o certificado é aceito e a comunicação continua. Caso a AC que assinou o certificado não conste na lista, o usuário é avisado e é dada a opção de incluí-la na lista de confiáveis. Desta forma, o

usuário torna-se responsável pela decisão de quais ACs são confiáveis. O controle da confiança é realizado pelo aplicativo, neste caso, o navegador (CERTISIGN, 2001).

Além de emitir os certificados, a AC tem a responsabilidade de garantir a identidade das entidades possuidoras do certificado durante uma comunicação (HOUSLEY e POLK, 1999).

Em resumo, os serviços oferecidos pela AC são:

- Emissão de certificados digitais e registro de chaves.
- Validação dos certificados emitidos.
- Gerenciamento de certificados digitais, cancelamento e revogação.
- Redirecionamento de certificados emitidos por outra certificadora digital.
- Revalidação de certificados vencidos e revogados.

- **Autoridade de Registro**

A Autoridade de Registro é o componente responsável pela conferência dos dados incluídos na requisição do certificado. Ela recebe uma requisição de assinatura de certificado e confere seus dados. Após a conferência, a requisição é assinada e repassada para a Autoridade Certificadora da comunicação (HOUSLEY e POLK, 1999).

- **Módulo Público**

É o componente responsável por fornecer uma interface para que o usuário possa fazer a solicitação de um certificado. Todas as funcionalidades de uma certificação estarão disponíveis neste módulo. O módulo público poderá conter também listas de certificados revogados e certificados de outras ACs (HOUSLEY e POLK, 1999).

- **Diretório Público**

É o componente responsável pela publicação dos certificados. Os certificados devem ser divulgados sem restrições. O diretório público pode armazenar, além de certificados de usuários, certificados de ACs e listas de certificados revogados. Ele deve

manter sempre os dados atualizados e manter um alto nível de disponibilidade das informações de comunicação (HOUSLEY e POLK, 1999).

2.2.2 Hierarquia

É a maneira pela qual uma Infra-estrutura de Chave Pública é organizada, podendo esta definir sua confiabilidade nas entidades. Cada organização possui uma denominação, de acordo com a maneira hierárquica que as Autoridades Certificadoras são arranjadas. Existem vários tipos de hierarquia. A mais usual é a hierarquia isolada, a qual é usada na ICP-Brasil. Este trabalho apresenta conceitos sobre algumas hierarquias, com ênfase na hierarquia isolada.

- **Hierarquia Isolada**

A hierarquia isolada é formada por uma Autoridade Certificadora no topo da hierarquia, um número indefinido de Autoridades Certificadoras intermediárias e as entidades finais.

A Autoridade Certificadora que fica localizada no topo da hierarquia é denominada Autoridade Certificadora Raiz (AC-Raiz). A AC-Raiz é auto-assinada, ou seja, seu certificado é assinado usando a própria chave privada. Abaixo dela pode haver vários níveis de ACs intermediárias, sendo de sua responsabilidade a decisão do número máximo de níveis. A AC-Raiz não deve emitir certificados para usuários finais. Quem faz essa emissão são as ACs intermediárias, que, além de certificados para usuários finais, mediante autorização da AC-Raiz, podem emitir certificados para outras ACs que estão localizadas abaixo delas. São considerados entidades finais os usuários, aplicações ou dispositivos que possuem certificados emitidos por uma das Autoridades Certificadoras intermediárias (ADAMS e LLOYD, 1999). A Figura 6 mostra um exemplo de hierarquia isolada.

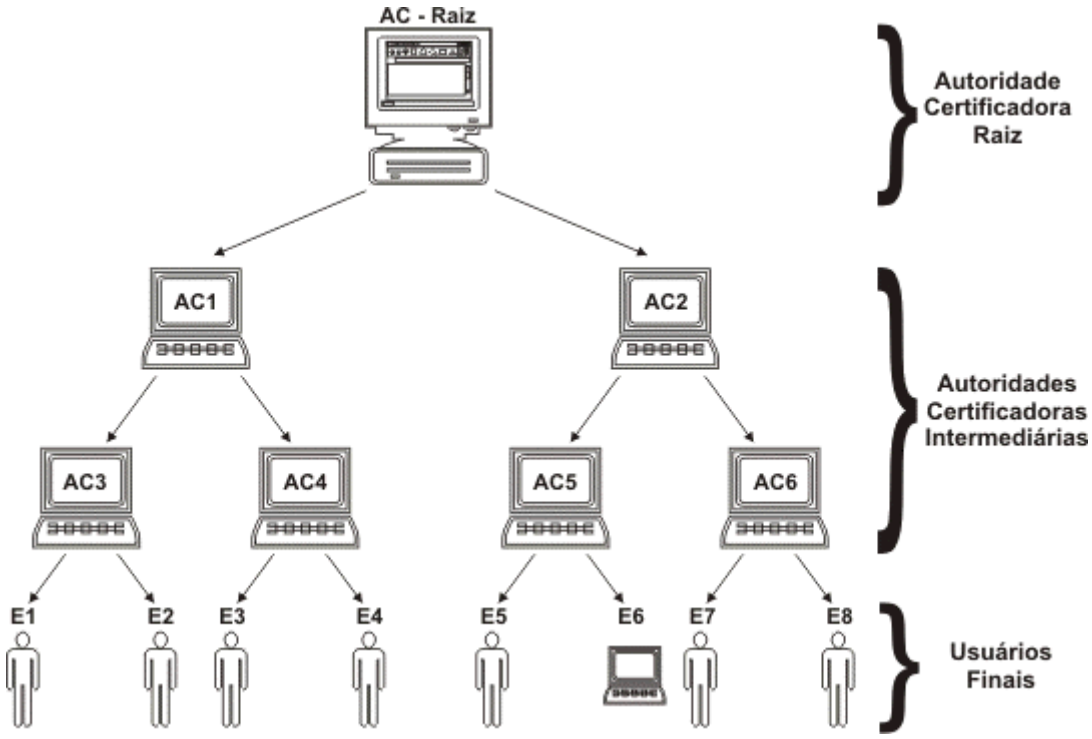


Figura 6 - Hierarquia Isolada

- **Certificação Cruzada**

Certificação cruzada é um mecanismo muito útil quando se deseja estabelecer a confiança entre duas ACs, em que cada uma possui sua hierarquia própria.

Os dois tipos de certificação cruzada serão descritos a seguir:

- Unilateral - Neste tipo de certificação cruzada somente um dos certificados é assinado pela outra AC, ou seja, a ACa assina o certificado da ACb, porém a ACb não assina o certificado da ACa.

- Mútuo - Envolve a assinatura dos certificados de ambas ACs, ou seja, a ACa assina o certificado da ACb, e esta assina o certificado da ACa.

A certificação cruzada pode ser utilizada para garantir a confiança entre duas Infra-estruturas de Chaves Públicas não ligadas. Através da certificação cruzada seria possível determinar a confiança para a validação de um certificado emitido por uma AC da ICPa em um sistema com certificado assinado por alguma AC da ICPb (ADAMS e LLOYD, 1999).

- **Floresta de Hierarquias**

Uma Floresta de Hierarquia é uma ligação entre várias ICPs distintas. Essas ICPs normalmente são hierarquias isoladas que necessitam estabelecer uma confiança com outras ICPs.

Para conectar essas hierarquias, é utilizado o mecanismo de certificação cruzada entre a AC-Raiz de uma hierarquia com a AC-Raiz da outra. Somente AC-Raízes devem utilizar certificação cruzada neste caso (ADAMS e LLOYD, 1999). Um exemplo de Floresta de Hierarquias é demostrado na Figura 7.

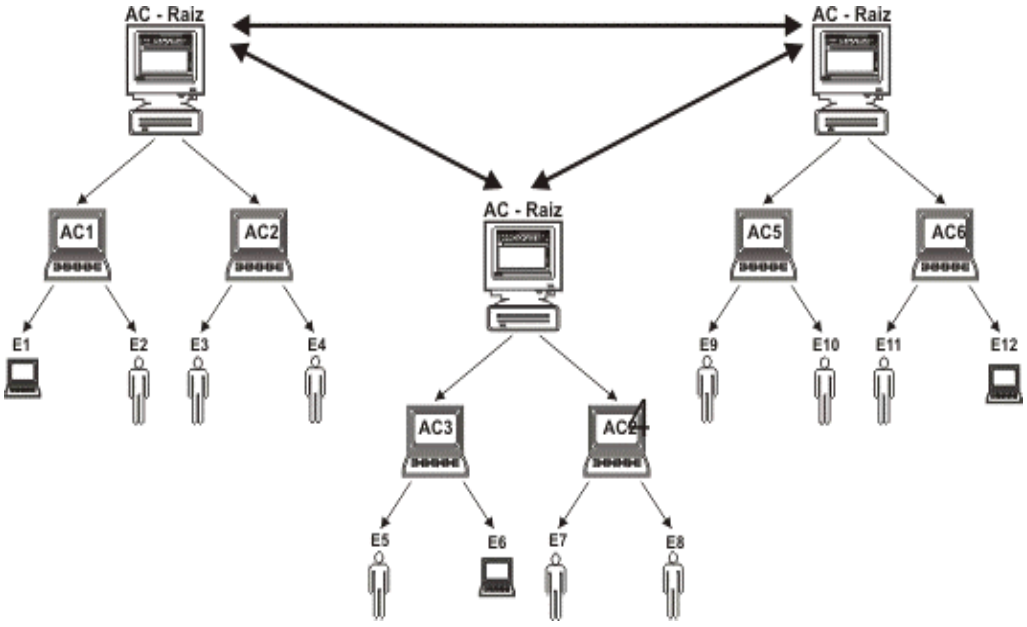


Figura 7 - Floresta de Hierarquias

- **Organização com Ponto Central**

Neste tipo de organização, cada ICP da Floresta possui uma certificação cruzada com uma infra-estrutura central, denominada Ponte. Ou seja, a ICP Central é o ponto de

ligação entre todas as ICP da Floresta (ADAMS e LLOYD, 1999). Uma estrutura utilizando uma ponte é ilustrada na Figura 8.

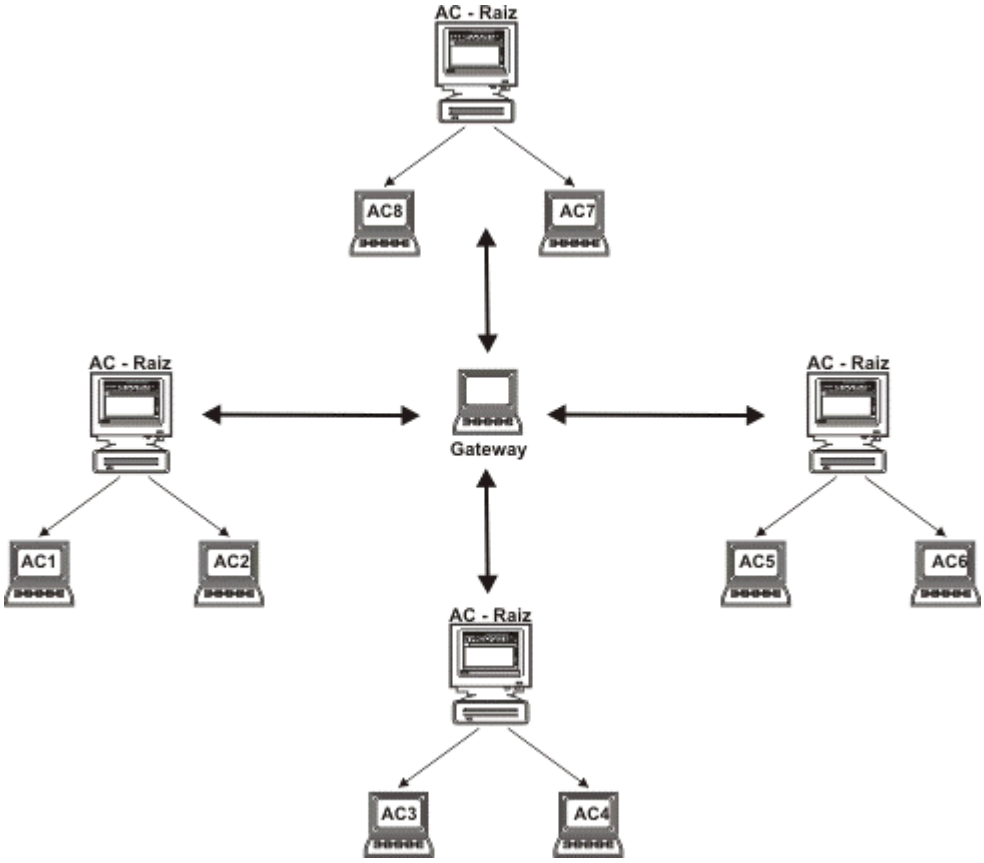


Figura 8 - Organização com Ponto Central

- **Modelo Internet**

Na Internet existem muitas ICPs localizadas em diversos lugares ao redor do mundo, utilizando hierarquias diferentes. Os navegadores criaram uma nova estrutura para atender as necessidades dos usuários das mais diversas ICPs.

Os navegadores trazem já instalados certificados de algumas AC-Raízes, consideradas confiáveis por eles. Assim, os usuários dessas ICPs possuirão uma confiança preestabelecida pelo navegador (ADAMS e LLOYD, 1999).

2.3 Norma ISO 17799

O aspecto segurança adquire cada vez mais importância no mundo dos negócios via redes eletrônicas. Assim, as empresas que querem sobreviver nesse ambiente tentam oferecer um alto nível de proteção durante as transações. Porém, muitas vezes a área de tecnologia da informação dessas empresas são vulneráveis a incidentes, o que coloca em risco suas operações. Na busca de uma solução, as organizações adotam procedimentos como o uso de produtos para proteger os ativos digitais e para controlar acessos definidos internamente. Para a garantia de bons resultados, é necessário implementar esses procedimentos seguindo uma orientação global. Um ponto de partida na implementação de um processo de segurança das informações é considerar o uso da norma ISO 17799.

A norma ISO 17799 é uma ferramenta disponível no mercado que busca melhorar a segurança digital das empresas. A norma traz 127 controles que permitem identificar vulnerabilidades, garantir segurança em todos os aspectos e a continuidade em seus negócios (INTERSIX, 2001). Para isso, devem ser utilizados produtos, como certificados digitais, *firewall*, sistema de controle de acesso etc. Porém, é preciso que os produtos sejam organizados conforme os controles da norma, oferecendo, assim, um nível máximo de segurança.

Serão apresentados a seguir todos os tópicos que fazem parte da norma. Não existe uma ordem para implementá-los e também não há a obrigatoriedade de que todos os tópicos sejam seguidos. A norma serve como uma orientação para a organização, que irá escolher os controles adequados ao seu tipo de negócio. Cada tópico a ser apresentado contém os dados completos e, por esse motivo, algumas informações serão repetidas em diferentes lugares.

2.3.1 Apresentação da Norma ISO 17799

- **Abrangência**

A norma ISO 17799 abrange todos os aspectos de segurança de uma organização, desde pessoas que trabalham na empresa até a parte lógica de segurança da informação, passando pela segurança física, de equipamentos, escritório e papéis. A norma está dividida em 12 tópicos assim definidos:

1 - Objetivo
2 - Termos e definições
3 - Política de segurança
4 - Segurança organizacional
5 - Classificação e controle dos ativos de informação
6 - Segurança em pessoas
7 - Segurança física e do ambiente
8 - Gerenciamento das operações e comunicações
9 - Controle de acesso
10 - Desenvolvimento e manutenção de sistemas
11 - Gestão da continuidade do negócio
12 - Conformidade

Cada um desses tópicos será apresentada de forma sucinta a seguir e uma representação gráfica da norma será apresenta no Anexo A.

- Objetivo

O objetivo da norma ISO 17799 é oferecer a estrutura e servir como um ponto de referência para as pessoas que são responsáveis por implantar e dar manutenção em segurança de uma organização. A norma oferece também controles para implantação de uma Política de Segurança com o propósito de garantir confiança no relacionamento entre as organizações. As recomendações descritas na norma devem ser selecionadas e usadas por uma organização, de acordo com a legislação e as regulamentações vigentes.

- Termos e definições

Este tópico apresenta os objetivos para os quais a norma foi construída. Um dos objetivos é definir os termos da segurança da informação numa organização. Outro é para que esta organização consiga, com o uso da norma, avaliar e gerenciar os riscos que ela corre com a pouca atenção quanto à segurança da informação.

Fazem parte deste tópico três itens principais:

- *Segurança da informação*

Este item apresenta os termos de segurança da informação que foram usados como base para criação da norma. Os termos são: confidencialidade, integridade e disponibilidade da informação. Para uma organização manter-se competitiva, proteger sua imagem e reputação diante de outras organizações e clientes, as informações nela contidas devem ser acessadas somente por pessoas autorizadas, além de ser mantidas na organização conforme sua versão original e estar disponíveis a usuários autorizados sempre que for necessário.

- *Avaliação de risco*

Avaliação de riscos pode ser definida como: estudo das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência. Com base nesses resultados, a organização faz uma avaliação da probabilidade de ocorrência de possíveis incidentes.

- *Gerenciamento de risco*

Gerenciamento de risco pode ser definido como: um processo de minimização ou eliminação dos riscos de segurança que poderão causar impacto tanto no aspecto financeiro quanto organizacional de uma empresa.

- Política de Segurança

Este tópico orienta sobre os procedimentos para implantar uma política de segurança em uma organização. É preciso definir uma política de segurança com termos claros que demostrem aos funcionários a preocupação e a importância da segurança para a organização. Os termos de implantação surgem em decorrência de uma análise crítica de risco dos pontos vulneráveis. Para cada vulnerabilidade existirão as respectivas ações a serem executadas. Esses termos devem ser documentados e aprovados pela direção da organização. O documento resultante desta etapa deverá ser publicado, comunicado e estar ao alcance de todos os funcionários de forma compreensível.

Nesta fase é preciso também designar um gestor, que será responsável pela manutenção e análise crítica da política definida. As análises críticas devem ser agendadas e executadas periodicamente e podem ser feitas extraordinariamente em decorrência de qualquer mudança que venha a afetar a avaliação de risco original, seja um incidente de segurança significativo, novas vulnerabilidades, mudanças organizacionais ou na infra-estrutura técnica.

De acordo com a norma, este é o tópico número 3 e está dividido nas seguintes partes:

3.1 - Política de segurança da informação
3.1.1 - Documento da política de segurança da informação
3.1.2 - Análise crítica e avaliação

- Segurança Organizacional

O objetivo deste tópico é orientar o gerenciamento da segurança organizacional. A segurança de uma organização é uma obrigação que deve ser compartilhada por todos os membros da direção. Recomenda-se criar um fórum com o objetivo de direcionar as obrigações e o comprometimento com os requisitos de segurança. É importante nomear um gestor que se responsabilize pela segurança geral da organização.

A política de segurança deverá fornecer um documento com procedimentos claros, contendo as regras e responsabilidades específicas para cada ativo, seja físico ou de informação. Uma prática adotada pelas grandes organizações é a indicação de um proprietário para cada ativo de informação. Essa pessoa fica responsável pela segurança do dia-a-dia de seu ativo. No entanto, o responsável final pela segurança é o gestor anteriormente nomeado, que é encarregado de verificar se as responsabilidades delegadas aos proprietários estão sendo executadas corretamente.

As organizações que desejam implantar de forma correta uma política de segurança deverão ter acesso a alguma consultoria especializada no assunto. Porém, o ideal é contratar um especialista em segurança. Caso não comportem esse especialista, as organizações deverão identificar um funcionário que, dentro de suas experiências, possa fornecer apoio nos aspectos de segurança e nas tomadas de decisão na área. Se este

colaborador não puder oferecer todo o apoio necessário, uma solução é contratar um consultor externo. A consultoria externa apresenta vantagens em função de sua experiência em trabalhos similares. Em caso de suspeitas de incidentes, o colaborador ou o consultor deve ser avisado imediatamente.

A segurança da informação aplicada deverá se submeter a análises críticas para garantir que as práticas definidas são adequadas às necessidades da organização. Essas análises podem ser executadas pela auditoria interna, por um gestor independente ou por organizações prestadoras de serviços.

A presença de prestadores de serviços na organização aumenta a fragilidade da segurança. Neste caso, é preciso fazer uma avaliação que identifique os riscos envolvidos, determinando as possíveis implicações na segurança e os controles necessários para garantir a segurança. Ambas as partes, empresa e prestadores, deverão estar em acordo sobre esses controles, firmando e assinando contratos sobre segurança. Em casos de envolvimento de outros participantes, convém que os contratos incluam, além dos controles, a permissão a essas pessoas e as condições de seu acesso às informações. Esses acordos deverão considerar os riscos, controles de segurança e procedimentos para os sistemas de informação, rede de computadores e/ou estações de trabalho.

Para que haja colaboração com a segurança da informação em uma organização, é necessário incentivar o uso das práticas de segurança entre os usuários, administradores, projetistas, enfim, todas as pessoas envolvidas direta ou indiretamente com a organização.

De acordo com a norma, este é o tópico número 4 e está dividido nas seguintes partes:

- 4.1 - Infra-estrutura da segurança da informação
  - 4.1.1 - Gestão do fórum de segurança da informação
  - 4.1.2 – Coordenação da segurança da informação
  - 4.1.3 – Atribuição das responsabilidades em segurança da informação
  - 4.1.4 – Processo de autorização para as instalações de processamento da informação
  - 4.1.5 – Consultoria especializada em segurança da informação
  - 4.1.6 – Cooperação entre organizações
  - 4.1.7 - Análise crítica independente de segurança da informação
- 4.2 - Segurança no acesso de prestadores de serviços

4.2.1 – Identificação dos riscos no acesso de prestadores de serviços
4.2.2 – Requisitos de segurança nos contratos com prestadores de serviços
4.3 – Terceirização
4.3.1 – Requisitos de segurança dos contratos de terceirização

- Classificação e controle dos ativos da informação

Este tópico tem o objetivo de auxiliar na manutenção e proteção dos ativos da informação e garantir que estes estejam recebendo um nível adequado de proteção. Para isso, é preciso fazer inventários dos principais ativos da organização. Cada ativo terá um proprietário nomeado para ser responsável por verificar se a segurança está sendo mantida de forma adequada, e também pela manutenção apropriada dos controles e a prestação de contas. A responsabilidade pela implementação dos controles pode ser delegada a outros gestores ou prestadores de serviços. Mas a prestação de contas fica a cargo do proprietário responsável pelo ativo.

As informações são classificadas quanto à sua importância e prioridade, pois elas possuem diferentes níveis de sensibilidade e criticidade. Algumas informações necessitam de um nível adicional de proteção ou um tratamento especial, outras não. Sendo assim, é preciso usar um sistema de classificação de informações para definir os níveis de proteção e determinar suas respectivas necessidades de medidas especiais de tratamento.

De acordo com a norma, este é o tópico número 5 e está dividido nas seguintes partes:

5.1 - Contabilização dos ativos
5.1.1 - Inventário dos ativos de informação
5.2 - Classificação da informação
5.2.1 - Recomendações para a classificação
5.2.2 - Rótulos e tratamento da informação

- Segurança em pessoas

O objetivo deste tópico é auxiliar na redução de riscos de erro humano, roubo, fraude e uso indevido das instalações. Busca também ajudar na conscientização dos

funcionários em relação a ameaças e a preocupações da organização com a segurança da informação, assegurando que eles estejam equipados para apoiar a política de segurança durante a execução normal do trabalho.

A seleção para o recrutamento de funcionários para executar trabalhos sensíveis é feita mediante uma análise minuciosa dos mesmos. A preocupação da organização com a segurança da informação deve ser apresentada ao funcionário na sua contratação. Nesse momento, os contratados recebem suas responsabilidades e ficam cientes de que as responsabilidades a eles atribuídas serão monitoradas durante a vigência do contrato de trabalho. A organização deverá ter um contrato contendo acordos de sigilo, a ser assinado pelos funcionários contratados e/ou prestadores de serviços. É importante também fornecer um treinamento conforme os procedimentos de segurança e uso correto das instalações de processamento, de forma a diminuir possíveis riscos de segurança.

Em casos de suspeita ou incidentes de segurança, os funcionários precisam notificar e solicitar os canais apropriados, ou seja, os colaboradores ou os consultores de segurança, o mais rapidamente possível. Conforme a notificação recebida, o colaborador ou o consultor coleta evidências e descobre a origem do incidente.

Baseando-se nos incidentes ocorridos, os responsáveis pela segurança notarão a necessidade de melhorias ou a adição de controles na política de segurança original. Assim, estarão aprendendo com os incidentes e se prevenindo contra ocorrências semelhantes. Os funcionários precisam estar cientes das medidas que serão tomadas pela organização em caso de incidentes provocados por eles.

De acordo com a norma, este é o tópico número 6 e está dividido nas seguintes partes:

- 6.1 – Segurança na definição e nos recursos humanos
  - 6.1.1 – Incluindo segurança nas responsabilidades do trabalho
  - 6.1.2 – Seleção e política de pessoal
  - 6.1.3 - Acordos de confidencialidade
  - 6.1.4 - Termos e condições de trabalho
- 6.2 – Treinamento dos usuários
  - 6.2.1 - Educação e treinamento em segurança da informação
- 6.3 – Respondendo aos incidentes de segurança e ao mau funcionamento
  - 6.3.1 - Notificação dos incidentes de segurança

6.3.2 - Notificando falhas na segurança

6.3.3 - Notificando mau funcionamento de software

6.3.4 - Aprendendo com os incidentes

6.3.5 - Processo disciplinar

- Segurança física e do ambiente

Este tópico apresenta uma orientação de como implementar e monitorar a segurança física de uma organização.

O primeiro passo a ser dado para a implementação de segurança física em uma organização é o estabelecimento de perímetros de segurança em torno das áreas que contenham as propriedades físicas, ou seja, estabelecer barreiras que controlem e impeçam a entrada de pessoas não autorizadas. Essas barreiras podem ser uma parede, uma porta com controle de entrada e saída baseado em cartões ou até mesmo um balcão com controle manual de entrada e saída.

Após essa etapa, será necessária a execução de minuciosas análises de riscos para se obter o nível de vulnerabilidade de cada ativo. Baseando-se no resultado da análise, é preciso definir controles de segurança proporcionais aos níveis de riscos identificados.

Os equipamentos também deverão receber proteção adequada para garantir: a redução de risco de acesso não autorizado; a proteção contra ameaças ambientais; a proteção contra falhas de energia ou falhas na alimentação elétrica; e a proteção no cabeamento que é responsável pela transmissão de dados e suporte de serviços de informação.

Algumas medidas de segurança serão necessárias, como: política de mesa limpa, para garantir a segurança de papéis e mídias removíveis; e política de tela limpa, para reduzir o acesso não autorizado, perdas ou danos à informação.

A retirada de equipamentos da organização só deverá ser possível com prévia autorização, e o equipamento retirado deverá ser conectado novamente assim que retornar. É necessário fazer inspeções freqüentes em toda organização, para identificar ausência não autorizada de propriedades.

De acordo com a norma, este é o tópico número 7 e está dividido nas seguintes partes:

7.1 - Áreas de segurança
- 7.1.1 – Perímetro da segurança física
- 7.1.2 – Controles de entrada física
- 7.1.3 – Segurança em escritórios, salas e instalações de processamento
- 7.1.4 – Trabalhando em áreas de segurança
- 7.1.5 – Isolamento das áreas de expedição e carga

7.2 – Segurança dos equipamentos
- 7.2.1 – Instalação e proteção de equipamentos
- 7.2.2 – Fornecimento de energia
- 7.2.3 – Segurança do cabeamento
- 7.2.4 – Manutenção de equipamentos
- 7.2.5 – Segurança de equipamentos fora das instalações
- 7.2.6 – Reutilização e alienação segura de equipamentos

7.3 - Controles Gerais
- 7.3.1 - Política de mesa limpa e tela limpa
- 7.3.2 – Remoção da propriedade

- Gerenciamento das operações e comunicações

Este tópico tem como objetivo auxiliar: na operação segura e correta dos recursos de processamento da informação; na diminuição de riscos de falhas nos sistemas; na proteção da integridade dos software e das informações; na manutenção da integridade e disponibilidade dos serviços de comunicação e processamento; na garantia da salvaguarda das informações da rede e na proteção da infra-estrutura de suporte; na prevenção de danos aos ativos causadores de interrupções das atividades do negócio; e na prevenção de perda, modificações ou mau uso de informações trocadas entre organizações.

É preciso que a organização tenha os procedimentos de operação documentados e atualizados. Estes procedimentos são considerados documentos formais. Em casos de necessidade de mudanças, estas somente poderão ser realizadas mediante autorização da direção. As modificações nos sistemas e recursos de processamentos deverão ser controladas. Para isso, convém definir procedimentos e responsabilidades que garantam um nível de segurança satisfatório.

No gerenciamento de incidentes, é preciso que os procedimentos e as pessoas responsáveis já estejam definidos. Em casos de incidentes, os responsáveis devem ter respostas rápidas, efetivas e ordenadas.

O método adotado pelas grandes organizações é o de segregação de funções, visando diminuir o risco de mau uso dos sistemas. Segregação de funções é um método que separa áreas de trabalho, dando direito ao uso de informações e serviços, somente a pessoas envolvidas nas respectivas áreas, ou seja, as pessoas que executam suas funções na área administrativa, poderão utilizar serviços e informações administrativos. A separação diminui as oportunidades de alterações não autorizadas no sistema ou uso incorreto dos serviços e das informações. Para se alcançar a segregação de funções, é preciso separar ambientes de desenvolvimento, produção e teste, para evitar que integrantes de um ambiente interfiram nos procedimentos de outro. Em casos de organização onde o gerenciamento do processamento seja feito por terceiros, ou seja, por prestadores de serviços, os riscos e os controles apropriados deverão ser identificados e acordados no contrato de serviço.

Convém estabelecer critérios para avaliar a aceitação de novos sistemas. Os gestores deverão efetuar testes em caso de novos sistemas, atualizações de versões e atualizações em geral. O objetivo é garantir que as mudanças não comprometerão a segurança e a continuidade do negócio.

Os gestores também são responsáveis pela implantação de controles especiais de detecção e prevenção contra introdução de softwares maliciosos. Os usuários precisam ser conscientizados das vulnerabilidades dos ambientes de processamento diante da introdução desses programas, que podem ser: softwares sem licença, vírus, cavalos de tróia e outros.

É importante implantar procedimentos de cópias de segurança e de disponibilização dos recursos de reserva, ou seja, as próprias cópias. Assim, em casos de incidentes, as informações podem ser restauradas e viabilizadas em tempo hábil.

Convém adotar controles de registro de operações e registro de falhas. As operações realizadas devem ser mantidas em registro contendo a data, a hora, a confirmação do tratamento correto das informações e a identificação de quem efetuou a operação. Em casos de falhas ocorridas durante a operação, é preciso registrá-las e tomar as providências de ações corretivas.

A proteção das informações que trafegam em redes públicas também precisam receber uma atenção especial. A meta é garantir que as informações não sejam acessadas por pessoas não autorizadas, e também assegurar a integridade e a autenticidade dos dados que estarão disponíveis na rede.

Procedimentos operacionais de proteção física deverão ser usados para proteger documentos e mídias magnéticas (fitas, discos, cartuchos) contra roubos, acessos não autorizados e danos em geral. É preciso que o descarte de mídias removíveis ou documentos seja feito de forma segura, principalmente quando se tratar de informações sigilosas. Nestes casos, recomenda-se o uso de procedimentos como incineração ou trituração.

Convém que as trocas de informações e softwares entre organizações sejam efetuadas com base em contratos, e que estejam em conformidade com toda legislação pertinente. Empresas que trabalham com comércio eletrônico precisam adotar controles para proteger-se das inúmeras ameaças que podem resultar em atividades fraudulentas, violações de contratos e divulgação ou modificações de informações. Uma política clara deve ser definida para a utilização do correio eletrônico.

De acordo com a norma, este é o tópico número 8 e está dividido nas seguintes partes:

8.1 - Procedimentos e responsabilidades operacionais
- 8.1.1 - Documentação dos procedimentos de operação
- 8.1.2 - Controle de mudanças operacionais
- 8.1.3 - Procedimentos para o gerenciamento de incidentes
- 8.1.4 - Segregação de funções
- 8.1.5 - Separação dos ambientes de desenvolvimento e de produção
- 8.1.6 - Gestão de recursos terceirizados

8.2 - Planejamento e aceitação dos sistemas
- 8.2.1 – Planejamento de capacidade
- 8.2.2 – Aceitação de sistemas

8.3 - Proteção contra software malicioso
- 8.3.1 – Controles contra software malicioso

8.4 – *Housekeeping*
- 8.4.1 - Cópias de segurança
- 8.4.2 – Registros de operação
- 8.4.3 – Registros de falhas

8.5 - Gerenciamento de rede
- 8.5.1 – Controles de rede

8.6 - Segurança e tratamento de mídias

8.6.1 – Gerenciamento de mídias removíveis

8.6.2 - Descarte de mídias

8.6.3 - Procedimentos para tratamento de informação

8.6.4 - Segurança da documentação dos sistemas

8.7 - Troca de informações e software

8.7.1 - Acordos para a troca de informações e software

8.7.2 - Segurança de mídias em trânsito

8.7.3 - Segurança no comércio eletrônico

8.7.4 - Segurança do correio eletrônico

8.7.5 - Segurança dos sistemas eletrônicos de escritório

8.7.6 - Sistemas disponíveis publicamente

8.7.7 - Outras formas de troca de informação

- Controle de acesso

Este tópico tem o objetivo de auxiliar a controlar o acesso lógico às informações. É preciso estabelecer procedimentos para esse controle, em especial os que analisem acessos privilegiados, ou seja, aqueles que permitam sobreposição, retiradas e alterações no sistema.

Esses procedimentos deverão cobrir todos os estágios do ciclo de vida dos usuários, desde o registro inicial até o final, que exclui os usuários que não necessitarão mais contatar o sistema. Trata-se de um cuidado que visa garantir que o sistema não fique disponível a usuários que não pertençam mais à organização. É importante também controlar o acesso à rede interna e externa. Para isso, existem alguns procedimentos a serem seguidos, como, por exemplo: uso de interfaces apropriadas entre a rede da organização e as redes públicas; uso de autenticação para usuários e equipamentos; e controle de acesso dos usuários aos serviços de informação. Isso garante que os acessos à rede não comprometam a segurança de seus serviços.

É preciso usar também as funcionalidades de segurança do sistema operacional, que permitem: identificação e verificação da identidade, do terminal e da localização do acesso; registrar os sucessos e as falhas de acesso ao sistema; fornecer meios apropriados de autenticação (que deve ser garantida com o uso de um gerenciamento de chaves e senhas de qualidade); e restringir o tempo de conexão dos usuários. Com base nos riscos do negócio, outros métodos de controle poderão ser disponibilizados mediante justificativa.

O acesso aos softwares aplicativos também deve ser controlado. Isso é feito conforme a política de controle de acesso já definida. Nela devem constar dois tipos de controle: o de permissão de acesso, em que a autorização de leitura, escrita, eliminação e execução de informações são fornecidas somente a usuários confiáveis; e o controle de saída das informações, em que só é permitida a saída de informações relevantes e estas só podem ser enviadas para locais autorizados. As saídas precisam se submeter a análises críticas periódicas, para a garantia da remoção de informações redundantes.

O controle de acesso deve ser monitorado, com o objetivo de detectar divergências entre a política estabelecida e os registros de eventos monitorados, bem como fornecer evidências no caso de incidentes de segurança. Outros casos que merecem atenção são os de computação móvel e de trabalho remoto. Na utilização de computação móvel, é preciso considerar os riscos de se trabalhar em um ambiente desprotegido; a proteção adequada deve ser aplicada. No trabalho remoto, este deve ser autorizado e controlado pelo gestor responsável na organização; também é preciso aplicar proteção no local do trabalho.

De acordo com a norma, este é o tópico número 9 e está dividido nas seguintes partes:

9.1 - Requisitos do negócio para controle de acesso
- 9.1.1 – Política de controle de acesso

9.2 – Gerenciamento de acessos do usuário
- 9.2.1 - Registro de usuário
- 9.2.2 - Gerenciamento de privilégios
- 9.2.3 - Gerenciamento de senha dos usuários
- 9.2.4 - Análise crítica dos direitos de acesso do usuário

9.3 – Responsabilidades do usuário
- 9.3.1 - Uso de senhas
- 9.3.2 - Equipamento de usuário sem monitoração

9.4 - Controle de acesso à rede
- 9.4.1 - Política de utilização dos serviços de rede
- 9.4.2 - Rota de rede obrigatória
- 9.4.3 - Autenticação para conexão externa do usuário
- 9.4.4 - Autenticação de nó
- 9.4.5 - Proteção de portas de diagnóstico remotas

9.4.6 - Segregação de redes

9.4.7 - Controle de conexões de rede

9.4.8 - Controle de roteamento

9.4.9 - Segurança dos serviços de rede

9.5 - Controle de acesso ao sistema operacional

9.5.1 - Identificação automática de terminal

9.5.2 - Procedimentos de entrada no sistema (*log-on*)

9.5.3 - Identificação e autenticação de usuário

- Desenvolvimento e manutenção de sistemas

O objetivo deste tópico é garantir que a segurança seja parte integrante dos sistemas de informação. Visa também auxiliar: na prevenção de perda, modificações ou uso impróprio dos sistemas de aplicações; na proteção da confidencialidade, autenticidade e integridade das informações; na condução dos projetos de tecnologia e nas atividades de suporte; e na manutenção da segurança dos software e da informação do sistema de aplicação.

Em casos de implantação de novos sistemas ou de melhorias dos já existentes, os requisitos de segurança devem ser considerados como um tópico do projeto. Ou seja, a segurança deve fazer parte do estudo, e seus requisitos precisam ser identificados, acordados, justificados e documentados antes de se desenvolver o sistema. É importante prever controles como trilhas de auditoria, ou seja, uma seqüência de procedimentos de monitoração e registro de atividades para a prevenção de uso impróprio dos sistemas. Em casos de informações consideradas sensíveis ou valiosas, poderão ser adotados controles adicionais.

Informações que são consideradas de risco devem ser protegidas com técnicas e sistemas criptográficos, como por exemplo: a criptografia, para a proteção da confidencialidades da informação; e a assinatura digital, para a proteção da autenticidade e integridade de documentos eletrônicos. Para garantir que o andamento dos projetos e das atividades de suporte estão se encaminhando seguramente, é preciso controlar o acesso aos arquivos do sistema. A manutenção da integridade dos mesmos deve ser atribuída ao usuário ou ao grupo de desenvolvimento a quem pertence o sistema de aplicação ou software. Os ambientes de desenvolvimento e suporte precisam ser rigidamente controlados. Para isso gestores responsáveis pelos sistemas de aplicação respondem também pela segurança do ambiente de desenvolvimento ou suporte. Eles são encarregados de garantir que todas as

modificações propostas sejam analisadas criticamente, comprovando que elas não irão comprometer a segurança do sistema ou do ambiente de produção.

De acordo com a norma, este é o tópico número 10 e está dividido nas seguintes partes:

- 10.1 – Requisitos de segurança de sistemas
  - 10.1.1 - Análise e especificação dos requisitos de segurança
- 10.2 – Segurança nos sistemas de aplicação
  - 10.2.1 - Validação de dados de entrada
  - 10.2.2 - Controle de processamento interno
  - 10.2.3 - Autenticação de mensagem
  - 10.2.4 - Validação dos dados de saída
- 10.3 – Controle de criptografia
  - 10.3.1 - Política para o uso de controles de criptografia
  - 10.3.2 – Criptografia
  - 10.3.3 - Assinatura digital
  - 10.3.4 - Serviços de não repúdio
  - 10.3.5 - Gerenciamento de chaves
- 10.4 – Segurança de arquivos do sistema
  - 10.4.1 - Controle de software em produção
  - 10.4.2 - Proteção de dados de teste do sistema
  - 10.4.3 - Controle de acesso a bibliotecas de programa-fonte
- 10.5 – Segurança nos processos de desenvolvimento e suporte
  - 10.5.1 - Procedimentos de controle de mudanças
  - 10.5.2 - Análise crítica das mudanças técnicas do sistema operacional da produção
  - 10.5.3 - Restrições nas mudanças dos pacotes de software
  - 10.5.4 - *Covert channels* e cavalo de Tróia
  - 10.5.5 - Desenvolvimento terceirizado de software

- Gestão da Continuidade do Negócio

Este tópico tem o objetivo de auxiliar na eliminação de interrupções do negócio, causadas por diversos tipos de falhas e resultando em danos graves à organização. Um plano de continuidade de negócio deve ser mantido, testado e considerado um controle importantíssimo, de forma a se tornar parte integrante de todos os outros processos gerenciais. Este plano analisa os riscos aos quais a organização encontra-se vulnerável, sejam eles desastres naturais, acidentes, falhas de equipamentos ou ações intencionais. Com o resultado desta análise, são definidas ações ou providências a serem tomadas para cada risco identificado. Assim, a organização pode reduzir a um nível aceitável a interrupção dos negócios.

No plano de continuidade do negócio é preciso implementar também planos de contingência, de forma a garantir que os processos do negócio possam ser recuperados dentro de uma escala de tempo definida. Deve-se testar os planos e treinar os funcionários para que, no caso de um incidente, eles estejam aptos a colocar as providências em prática. Cada plano deve ter um responsável. Em casos de ausência temporária desse responsável, o plano é atualizado com os dados do substituto. Em casos de ausência definitiva do responsável, seus dados são substituído no plano. O plano precisa ser mantido por análises críticas regulares e consequentemente atualizações, para garantir sua contínua efetividade.

Este tópico é o principal alvo deste trabalho e será abordado com mais profundidade item 2.4.

De acordo com a norma, este é o tópico número 11 e está dividido nas seguintes partes:

11.1 - Aspectos da gestão da continuidade do negócio
- 11.1.1 - Processo de gestão da continuidade do negócio
- 11.1.2 - Continuidade do negócio e análise do impacto
- 11.1.3 - Documentação e implementação de planos de continuidade
- 11.1.4 - Estrutura do plano de continuidade do negócio
- 11.1.5 - Testes, manutenção e reavaliação dos planos de continuidade do negócio

- Conformidade

O objetivo deste tópico é auxiliar a evitar a violação de leis criminais ou civis, estatutos, regulamentações ou obrigações contratuais. Visa também auxiliar na garantia da conformidade dos sistemas com as políticas e normas organizacionais de segurança, bem como apoiar a auditoria de sistemas.

Para definir os requisitos de segurança, é importante contar com organizações de consultoria jurídica ou profissionais liberais adequadamente qualificados. O objetivo é garantir que os projetos, as operações, o uso e a gestão de sistemas estejam dentro dos requisitos de segurança corretos. Deve-se levar em consideração que os requisitos legislativos variam de um país para outro e também que informações criadas em um país são transmitidas a outros. A segurança dos sistemas de informação deve ser analisada criticamente tomando por base as políticas de segurança apropriadas. Além disso, a análise precisa ser feita em intervalos de tempo regulares, de modo a garantir que os sistemas de informação estão sendo adequadamente comparados com as normas de segurança anteriormente definidas.

As ferramentas de auditoria usadas para a checagem dos sistemas operacionais devem conter controles de segurança, a fim de evitar uso impróprio e interrupção durante as atividade de auditoria. Elas devem estar separadas de sistemas em desenvolvimento e mantidas em áreas as quais somente usuários autorizados tenham acesso.

De acordo com a norma, este é o tópico número 12 e está dividido nas seguintes partes:

12.1 - Conformidade com requisitos legais
- 12.1.1 - Identificação da legislação vigente
- 12.1.2 - Direitos de propriedade intelectual
- 12.1.3 - Salvaguarda de registros organizacionais
- 12.1.4 - Proteção de dados e privacidade da informação pessoal
- 12.1.5 - Prevenção contra uso indevido de recursos de processamento da informação
- 12.1.6 - Regulamentações de controles de criptografia
- 12.1.7 - Coleta de evidências

12.2 - Análise crítica da política de segurança e da conformidade técnica
- 12.2.1 - Conformidade com a política de segurança

2.4 Plano de Continuidade de Negócios

As tecnologias disponíveis atualmente oferecem novas fontes de comercialização, aumentando os horizontes empresariais. Com o surgimento de empresas comercializando seus produtos pela Internet, originaram-se novas expectativas de mercado e novas vulnerabilidades. Essas vulnerabilidades podem ser no âmbito operacional ou natural. Porém, o número de negócios perdidos em razão da paralisação de um sistema, seja por motivo operacional ou não, causa um impacto financeiro enorme, além de prejudicar a imagem da empresa perante clientes e outras empresas (SALDANHA, 2000).

Por esses motivos, os empresários do meio cibernético estão revendo os antigos conceitos de prioridades. Estão considerando o Plano de Continuidade de Negócios uma medida de grande importância diante de todas as outras decisões de segurança adotadas por eles.

Uma medida que vem sendo usada para resolver problemas de reativação do negócio é o Plano de Contingências (PC). Trata-se de um plano desenvolvido para contingenciar situações diante de cenários desagradáveis, concentrado em ações específicas voltadas aos problemas de automatização. A responsabilidade de elaboração e execução do PC é atribuída ao departamento de Tecnologia da Informação (TI) isoladamente. Mesmo desempenhando um papel importante para a continuidade do negócio, o TI por si só não pode determinar quais processos são vitais para a organização nem definir a disponibilidade financeira a ser aplicada na proteção destes recursos (IBM, 2001).

Enquanto um PC se concentra em ações específicas, o Plano de Continuidade de Negócios é completo, abrange todos os processos da empresa e conta com a colaboração de todos os departamentos. Assim, oferece à organização a capacidade de cumprir seu papel diante dos clientes, mesmo durante um período de perturbações, permitindo ao negócio voltar ao andamento normal de uma forma equilibrada (BEAL, 2001).

O fator crucial que interliga o conceito de um PC com o de um PCN é a segurança. Ambos planejam estrategicamente garantias reais de conservação do atendimento ao cliente. Porém, um PCN bem elaborado inclui o PC como parte integrante.

Segundo Alevate (2001), falar em Plano de Contingência e em Plano de Continuidade de Negócios é falar em sobrevivência mercadológica.

2.4.1 Conceito de PCN

Segundo Marinho (2001), o Plano de Continuidade de Negócios é um planejamento de respostas feito antecipadamente ao acontecimento de possíveis ameaças. Este planejamento minimiza ou elimina a paralisação dos principais processos de negócios de uma empresa, o que ocasionaria impactos relevantes.

O PCN é uma medida preventiva de segurança, capaz de garantir a estabilidade e a manutenção das atividades na prestação de serviços de uma empresa. É o planejamento da recuperação de processos organizacionais críticos ocorridos logo após uma situação de dano à propriedade. Esses danos podem variar de acordo com a causa, que pode ser um incêndio, uma inundação ou uma simples falha técnica no sistema operacional (BEAL, 2001).

O PCN é, na verdade, uma forma de garantir a continuidade no atendimento ao cliente, isto é, não está restrito ao sistema automatizado de uma empresa. O plano aborda o planejamento estratégico de medidas preventivas para a resolução de outros problemas considerados de igual prioridade para a sobrevivência de um negócio. Um bom exemplo a ser dado é o incêndio na Estação da Barra da Tijuca da Telemar no Rio de Janeiro ocorrido em 1999. A empresa partiu do princípio de que a necessidade de seus clientes era a comunicação. Para solucionar o problema e suprir essa necessidade, aplicou como contingência o fornecimento de telefones celulares para os clientes com maior urgência, garantindo, assim, a continuidade do atendimento ao cliente. Isso conseqüentemente reflete na continuidade do negócio (SALDANHA, 1999).

O ponto de partida para a elaboração de um PCN é um estudo profundo sobre a empresa em questão. São destacados os processos e componentes críticos e vitais para a existência de um negócio e são previstos os possíveis acontecimentos desagradáveis.

Vários fatores merecem destaque na elaboração de um sistema para solucionar os desajustes em um período de perturbação: problemas do departamento de TI, departamento pessoal, departamentos de comunicações, acomodações de escritório, documentos vitais

impressos em papel etc. Esses fatores devem ser analisados e considerados de igual valor, para que o resultado do plano seja satisfatório. Em caso de ocorrência de incidentes, devem proporcionar tranqüilidade no retorno às atividade normais do negócio.

No Manual de Planejamento da Continuidade do Negócio (BEAL, 2001), o objetivo principal da elaboração e manutenção de um PCN é a busca da permanência da integridade dos dados organizacionais, juntamente com instalações de processamento e serviço operacional. Caso haja necessidade, um serviço temporário ou restrito é usado, até que o serviço normal possa ser recuperado (BEAL, 2001).

O sucesso de um PCN exige uma combinação de competências, habilidades e conhecimentos que envolvem o ambiente organizacional. Ou seja, deve-se conhecer as necessidades a serem supridas, as estratégias, as formas viáveis de solução. Cada item exige uma análise cautelosa e criteriosa do panorama dos riscos que ameaçam a organização. A escolha das alternativas viáveis para o gerenciamento de cada ameaça deve pautar-se na relação custo/benefício, visando resultados palpáveis e capazes de garantir a estabilidade do processo.

O intuito primordial do PCN gira em torno de uma ação capaz de otimizar planos projetados para reduzir ao máximo as perdas organizacionais. Assim, todas as providências e decisões devem ser adotadas de forma que a agilidade possa evitar ou diminuir cenários desastrosos.

O plano deve seguir uma ordem hierárquica de prioridade. Cada instância precisa ter um responsável devidamente identificado, ou seja, um gerente para prestar contas ao Conselho Diretor quanto à manutenção de um plano de continuidade de aplicação viável. Caso não haja alguém que responda pela execução de determinadas tarefas, a probabilidade de insucesso aumenta.

Todo PCN deve ser constituído de várias etapas e cada etapa irá conter várias instâncias. Cada instância deve ser supervisionada por um comitê responsável pelo controle geral e pela análise do processo evolutivo alcançado ao final de cada etapa. Os dados de identificação das pessoas responsáveis pelas instâncias deverão ser incluídos e considerados como parte essencial do plano. Esses dados devem conter o endereço, telefones etc. É importante salvar essas informações em vários lugares, para que haja rapidez na busca de soluções.

2.4.2 Etapas de um PCN

Este tópico traz a descrição das etapas de um PCN. Toma-se por base o Manual de Planejamento da Continuidade de Negócio (BEAL, 2001), que traz um planejamento genérico e adaptável a qualquer ramo de atividade.

- **Análise do Impacto Organizacional**

Esta é a primeira etapa de um PCN e nela é feita a leitura detalhada, avaliativa e criteriosa de cada sistema organizacional. O objetivo é identificar os impactos que uma interrupção de seu funcionamento causaria à organização e, conseqüentemente, sua importância para as atividades da empresa ou negócio. Esta análise deve levantar todos os pontos críticos, a fim de que os controles possam ser melhorados e os riscos, reduzidos.

A análise do impacto organizacional busca identificar os sistemas organizacionais e classificá-lo por ordem prioritária, para o pronto atendimento de uma gerência eficaz.

Duas categorias fazem parte da análise do impacto organizacional:

- Impactos quantificáveis.
- Impactos não quantificáveis.

- **Impactos quantificáveis**

Os investimentos em procedimentos que se enquadram nesta categoria deverão ser justificados, pois serão expressos em termos financeiros. Esses impactos podem ser:

- Perdas financeiras - por exemplo, o custo na reposição de um ativo destruído, ou melhor, o gasto para reposição de um patrimônio que rendia a produtividade.
- Diminuição da receita - menor fluxo de vendas, dificuldade de controle de dívidas a receber, necessidade de empréstimos para repor perda de patrimônio.
- Aumento de custo de trabalho - necessidade de maior produtividade para a manutenção da receita, aumento dos custos obrigatórios para a continuidade do negócio.
- Penalidades financeiras - descumprimento de contratos e acordos comerciais, fracasso em manter as metas definidas em acordos em nível de serviço ou multas aplicadas.

- **Impactos não quantificáveis**

São impactos considerados difíceis de ser traduzidos em valor monetário:

- Perda de reputação.
- Perda de credibilidade.
- Embaraços políticos, corporativos ou pessoais.
- Descumprimento da lei.
- Riscos para a segurança pessoal dos envolvidos.
- Perda da capacidade operacional de produção.

Após efetuada essa análise e tendo a abstração dos sistemas vitais para a organização, a próxima etapa é atribuir a eles um prazo de recuperação.

- **Prazo de Recuperação**

Nesta fase serão determinados os prazos de recuperação dos sistemas. Após a análise e classificação dos processos de negócio, considerando os impactos organizacionais, é necessário categorizar cada processo anteriormente definido em ordem de importância para a organização. Os sistemas deverão ser listados em ordem de importância. Se forem em grande quantidade, deverão se enquadrar dentro das seguintes categorias:

- Categoria 1 - devem ser recuperados dentro de n minutos.
- Categoria 2 - devem ser recuperados dentro de n horas.
- Categoria 3 - devem ser recuperados dentro de n dias.
- Categoria 4 - devem ser recuperados dentro de n semanas.
- Categoria 5 - importância varia de acordo com a data de vencimento (folha de pagamento, pagamento de fornecedores etc.).
- Categoria 6 - aplicações não críticas.

- **Medidas de Redução do Risco**

As medidas de redução de risco constituem o novo passo para a elaboração do PCN. Nesta fase deverão ser identificadas as áreas cuja probabilidade de risco é maior. Podem ser implementados nessas áreas controles adicionais mais óbvios para a garantia da redução de riscos e a prevenção de desastres. São considerados controles adicionais mais óbvios os procedimentos de manutenção e reparo de hardware, mecanismos de prevenção e detecção de incêndios, controles de acesso físico, entre outros.

- **Relatório para a Gerência**

O relatório para a gerência personaliza o resumo da trajetória de quanto a organização teria a perder no caso de desastre ou outro incidente, e com que rapidez essas perdas poderiam aumentar. O relatório deverá conter os processos mais vulneráveis para a organização (aqueles mais significativos para a empresa), classificados em ordem e grau de importância, bem como as caracterizações para cada um, que podem ser:

- A forma que o dano ou a perda poderá assumir.
- O nível de gravidade da perda ou dano no transcorrer do tempo após o incidente.
- As condições mínimas de pessoal, instalações e serviços necessários para se recuperar um nível de serviço de emergência.
- Tempo máximo tolerável tanto para a tomada de medidas quanto para a resolução do problema.

A identificação e a classificação dos sistemas organizacionais considerados sensíveis deverão ser aprovadas pela comissão designada para a supervisão do projeto.

- **Análise das Opções e Definição da Estratégia de Recuperação**

A segunda etapa do PCN corporifica a análise das opções de recuperação, que objetiva identificar e estimar os custos de ações viáveis para a recuperação de cada sistema que deve ser coberto pelo planejamento.

Na avaliação dos pontos básicos à prevenção de desastres, devem ser considerados os seguintes controles:

- Sistemas de detecção de intrusos, com o objetivo de controlar o acesso a localidades, edifícios.
- Equipamento de detecção e extinção de fogo.
- Controle de áreas de risco (como os que armazenam material inflamável).
- Proteção de registros vitais não magnéticos (documentos, microfilmes).
- Profissionais capacitados para substituição (em casos de necessidade).
- Arranjos para manutenção de equipamento em bom estado de conservação.
- Cópias-reserva de armazenamento e recuperação de sistemas computacionais e dados.

- **Cópias-reserva**

A estratégia de cópias-reserva é um recurso alternativo para resolução de problemas e constitui a garantia da vitalidade de todo e qualquer PCN.

"A característica principal de qualquer plano de continuidade de negócio é a estratégia de cópias-reserva. Se estas não existirem, não puderem ser acessadas ou recuperadas, nenhum planejamento de continuidade será bem sucedido" (BEAL, 2001).

As cópias-reserva devem estar sempre atualizadas, armazenadas remotamente e em locais de fácil acesso.

- **Recuperação do sistema**

Antes do acontecimento dos incidentes deverão ser efetuados testes de recuperação dos sistemas. Deve-se simular um acontecimento real, em que os dados necessitam ser recuperados em um tempo restrito e as cópias-reserva serão usadas em um ambiente que não seja de pleno conhecimento dos funcionários. Desta forma, a recuperação dos dados será testada para a validação do método.

É importante ressaltar que o PCN é uma visão estratégica política capaz de apontar e elaborar soluções de segurança em caso de interrupção de negócios, seja num contexto tecnológico ou não.

- **Desenvolvimento do Plano de Continuidade**

O desenvolvimento do PCN é o estágio em que é feito o detalhamento do plano. São tomadas decisões como a solicitação de coberturas de seguro. Além disso, as medidas de redução de riscos são implementadas e é definida uma administração para efetuar a manutenção e teste periódicos do plano.

O conteúdo de um PCN irá variar de acordo com a organização. Porém, todos os planos deverão apresentar informações detalhadas para cada um dos itens descritos abaixo:

- Administração da continuidade.
- Contratos de suporte.
- Operações computacionais.
- Infra-estrutura de TI.
- Unidade remota de armazenamento.
- Pessoal.
- Localidade principal.
- Localidade reserva.
- Retorno à normalidade.
- Requisitos de suporte.
- Remoção de pessoal.
- Restabelecimento dos serviços de apoio.
- Salvamento.

Todos esses itens devem ser considerados para o sucesso na elaboração desta etapa.

- **Treinamento e Conscientização do Pessoal**

Após a término do desenvolvimento do PCN, todas as pessoas que fazem parte da organização deverão ser conscientizadas. Isso é feito por meio de um treinamento envolvendo todos os membros da organização, mesmo aqueles que não tenham um papel específico no plano. O treinamento deverá informar pontos básicos do plano, a razão para a existência de um PCN, os procedimentos que deverão ser executados em casos de desastres, para onde eles devem se dirigir, quem deve ser solicitado etc.

O PCN perderá seu valor caso seu conteúdo não seja de conhecimento de todos os funcionários da organização.

- **Teste e Atualização do Plano**

A atualização do plano e o teste de eficiência garantem a confiabilidade do PCN.

O plano deverá submeter-se a atualizações periódicas, que visam assegurar que ele esteja acompanhando a situação atual da organização. Conseqüentemente, após a atualização, o plano deverá ser testado, de forma a garantir que os funcionários estejam conscientes em relação às suas responsabilidades e que estejam aptos a desempenhar seus papéis.

As vantagens que o PCN pode trazer fazem vislumbrar uma rota segura dos negócios no mundo empresarial.

CAPÍTULO III
METODOLOGIA SIMPLIFICADA

3.1 Justificativa

Atualmente as organizações encontram-se cercadas por uma grande quantidade de informações, em função dos recursos de Tecnologia da Informação disponíveis. O custo para obtenção, tratamento, guarda, disseminação e proteção dessas informações é alto.

Os mecanismos de segurança cada vez mais sofisticados não asseguram total proteção às informações. Desse modo, as organizações ficam expostas a riscos de intrusões, alterações, destruição, divulgação indevida, entre outros ataques.

Este trabalho foi desenvolvido com o objetivo de apresentar uma contribuição para a solução desse tipo de problema. Inicialmente foram apresentadas fundamentações sobre as técnicas utilizadas para garantir segurança, como, por exemplo, criptografia, função Hash e assinatura digital. Com o conhecimento dessas técnicas, pode-se entender o funcionamento dos certificados digitais, que é atualmente o método mais procurado por organizações que visam a segurança de suas informações. Os certificados digitais são emitidos por empresas chamadas Infra-estrutura de Chave Pública (ICP). Em razão da alta responsabilidade inerente aos serviços oferecidos por essas empresas, o grau de segurança das informações nelas contidas é grande.

Uma contribuição significativa para a padronização dos requisitos de segurança e para a elaboração da proposta deste trabalho é a norma ISO 17799. A norma é composta por diversos itens, porém todos com a mesma função: a segurança da informação.

Outro aspecto importante para organizações que prestam serviços de segurança a outras empresas é garantir a continuidade dos seus negócios. Dessa forma, é possível assegurar com segurança a continuidade do atendimento aos clientes. Assim, o presente trabalho também apresenta conceitos e etapas de como elaborar um Plano de Continuidade de

Negócios. Um Plano de Continuidade de Negócios (PCN) prepara as empresas para enfrentar situações desagradáveis com mais facilidade, caso elas venham a acontecer.

A metodologia apresentada neste capítulo é um procedimento a ser executado antes da elaboração de um PCN. A meta é auxiliar as empresas a saber quais são os riscos em potencial.

A Figura 9 ilustra a abrangência do trabalho e apresenta em destaque a Metodologia para Análise de Segurança - M.A.S:

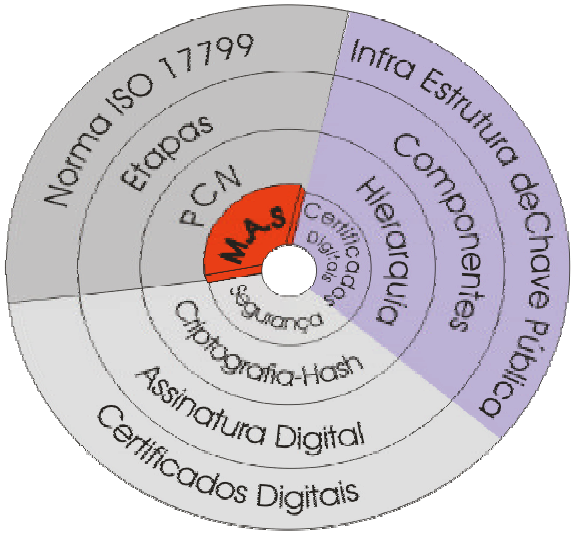


Figura 9 – Abrangência do Trabalho

Para a elaboração da M.A.S., foram realizadas várias pesquisas sobre os assuntos apresentados. Uma fonte bastante utilizada foi a Internet, que disponibiliza vários debates e experiências já realizadas na área de segurança da informação, além de fornecer indicações de literatura sobre o assunto.

No campo da Segurança da Informação, mais especificamente sobre Plano de Continuidade de Negócios, uma série de autores aborda a questão. Andrew Hiles e Peter Barnes, no livro “The Definitive Handbook of Business Continuity Management”, apresentam formas de visualizar a necessidade de elaborar um plano de segurança e como colocá-lo em prática. J. Barnes, em seu livro "A Guide to Business Continuity Planning", apresenta um guia para a elaboração de um Plano de Continuidade de Negócios.

Na obra "Comprehensive Information Security Policies" a Eon Commerce Limited trata de uma grande área da segurança e usa como referência a norma ISO 17799.

Conforme apresentado no item 3.1 deste capítulo, esta norma foi estudada e utilizada como apoio para a elaboração do M.A.S.

Como referência para o desenvolvimento deste trabalho, optou-se pelo livro de Saldanha (2000), “Introdução a Planos de Continuidade e Contingência Operacional”. Vários fatores contribuíram para a escolha desta literatura. Um deles é que o livro utiliza a norma ISO 17799 como ferramenta, enfocando exatamente os objetivos deste trabalho. Outra razão é que os conceitos e idéias apresentados no livro não são inovações, e sim estão baseados em métodos e procedimentos adotados nos EUA e preconizados pelo DRI – *Disaster Recovery Institute International*. A vasta experiência do autor na implantação de planos de segurança, a grande quantidade de publicações de artigos sobre o assunto e a facilidade de obtenção do material a um custo acessível também foram fatores que influenciaram na escolha desta literatura.

Saldanha (2000), apresenta em sua obra uma metodologia bastante complexa e detalhada para elaboração de uma Plano de Continuidade de Negócios. A metodologia utiliza diferentes análises e considera custos para gerar o resultado, além de propor alguns modelos de formulários e apresentar um questionário extenso com aproximadamente 400 perguntas baseadas no norma ISO 17799. Devido a abrangência da metodologia de Saldanha, sua aplicabilidade requer pessoas que possuam grande conhecimentos da empresa e da própria metodologia, dificultando desta forma, o uso da mesma por empresas de pequeno porte.

A M.A.S oferece flexibilidade e simplicidade em sua aplicação, contribuindo para a segurança das pequenas empresas. É importante salientar que as contribuições pessoais inseridas neste capítulo não estão referenciadas.

3.2 Metodologia

A segurança deixou de ser um diferencial usado pelas empresas para se destacar no mercado e passou a ser um fator crucial para a continuidade dos negócios. Por esse motivo, as empresas contam hoje com serviços prestados por consultores de segurança. Esses profissionais analisam a situação de segurança atual e, com base nesses dados, planejam estratégias para que, em caso de acontecimentos indesejáveis no futuro, a organização possa retornar à situação normal em tempo aceitável e não prejudicial a continuidade dos seus negócios. Para maior eficiência na elaboração deste planejamento, a organização já precisa

dispor de um nível básico de segurança. A partir deste nível básico, os consultores poderão planejar as estratégias de segurança com maior tranqüilidade.

Neste trabalho, a metodologia proposta foi direcionada à Infra-estrutura de Chave Pública - ICP, por ser um tipo de empresa que necessita de um alto nível de segurança. No entanto, é um método que pode ser aplicado em empresas de outros ramos.

A metodologia é composta por etapas que permitirão organizações, especificamente a ICP utilizada para teste, fazer uma auto-avaliação para alcançar um nível aceitável de segurança em um curto espaço de tempo e sem grandes investimentos. A abrangência da metodologia será apresentada de forma gráfica no Anexo B.

Em uma das etapas da metodologia, um questionário aborda os principais itens a serem avaliados em um trabalho de diagnóstico de uma empresa do tipo ICP. Mas a metodologia não esgota os requisitos de segurança, podendo ser adaptada com a inclusão ou eliminação de questões que se aplicam ao caso de empresas de outro ramo de atividade.

A aplicação das etapas pode ser feita por integrantes da própria organização que está sendo avaliada. Para alcançar bons resultados, é necessário que as etapas sejam seguidas e executadas por grupos de trabalho aptos a descreverem os processos e tomar decisões. Os grupos de trabalho que devem aplicar as etapas são:

- Grupo responsável pela condução do trabalho como um todo, ou seja, encarregado de coordenar e aplicar a metodologia. Deve conduzir o trabalho, atribuir as etapas aos respectivos grupos e gerar o resultado final.
- Grupo constituído pelos representantes e gestores de cada processo. Será responsável pela descrição do funcionamento dos processos realizados pela organização, suas dependências e também por responder um questionário. É importante que este grupo tenha conhecimentos profundos dos processos, para que possa responder com exatidão o questionário e levantar as vulnerabilidades existentes nos processos.
- Grupo constituído por representantes da administração da empresa. Será responsável por definir a cultura na organização, ressaltando quais são as preocupações e o grau de importância de cada uma. Este grupo deve ser formado por pessoas que tenham conhecimento e autonomia para decidir quais são os impactos mais relevantes e seu nível de importância.

As etapas da metodologia proposta são:

Metodologia simplificada para Análise de Segurança

Na etapa da Análise de Impacto, a metodologia que será utilizada é uma espécie de “pente fino”, ou seja, um detalhamento minucioso em todas as unidades da organização. A Análise de Impacto deve ser executada em uma unidade de cada vez. Dessa forma, o resultado será mais consistente, apresentando a descrição da unidade como um todo, porém realizada em partes separadas. Conforme Saldanha (2000), em cada unidade organizacional é preciso analisar os processos produtivos, pois sua perfeita continuidade é o alvo do trabalho. Nesta etapa serão levantados os impactos mais significativos para a organização.

Após a Análise de Impacto, cada um dos impactos classificados como importantes são submetidos à atribuição de valores, conforme o grau de importância. Os impactos importantes, ou seja, os que recebem maior valor, servem de base para identificar os processos que não poderão sofrer paralisações e suas dependências. Após identificados, os processos são representados por fluxogramas, que ilustram o funcionamento e as dependências entre eles.

O grupo de trabalho responsável ou os envolvidos nos processos responderão um questionário para levantar as vulnerabilidades existentes nos processos. Este procedimento pertence à etapa de Análise de Risco.

Considerando os resultados obtidos pela Análise de Impacto com seus respectivos valores, e as respostas obtidas no questionário na etapa Análise de Risco, a metodologia mostrará a situação atual da organização e quais as vulnerabilidades que precisam ser tratadas com mais urgência. Serão utilizados gráficos para a ilustrar os resultados obtidos pela intersecção das duas análises.

Neste trabalho, a metodologia será testada em uma Infra-estrutura de Chave Pública. Trata-se de sua utilização somente no nível de teste de aplicabilidade da metodologia. Optou-se por escolher uma empresa que atua nesse ramo de atividade, pois sua caraterística é a necessidade de possuir um alto nível de segurança, já que seu compromisso é garantir a segurança de outras empresas. As Infra-estruturas de Chaves Públicas são organizações que têm como principal objetivo a emissão de certificados digitais. Um dos principais serviços garantidos pelo uso de certificados digitais é a segurança em transações eletrônicas, fator que ainda causa polêmica entre os usuários de *e-commerce*. Assim, a metodologia testada em uma organização que necessita trabalhar sobre um alto nível de segurança testará a validade e a robustez da mesma.

3.3 Análise de Impacto

A Análise de Impacto Organizacional, segundo Saldanha (2000), pode ser definida como o trabalho que deverá identificar os impactos de um possível desastre sobre as operações de uma organização. Quanto maior o impacto decorrente da paralisação de um processo, mais crítico ele será.

Existem outras definições para Análise de Impacto Organizacional que, embora tenham o mesmo significado, destacam pontos diferentes. Estas definições serão mencionadas a seguir.

Segundo o OIC (Divisão de Segurança de Tecnologia de Informação da RCMP do Canadá), o objetivo final da análise de impacto é obter o apoio dos diversos participantes, fornecer insumos para a tomada de decisões e recomendar medidas preventivas (SALDANHA, 2000).

Segundo Michael (apud SALDANHA, 2000), esta etapa pode ser considerada como a revisão e análise de todas as unidades da organização para determinar o nível de risco e para definir a prioridade de recuperação na ocorrência de um desastre.

Segundo o Business Continuity Education Services da Strohl Sistems, é um processo contínuo de análise das funções de uma unidade organizacional, visando identificar o impacto de sua paralisação por um determinado período de tempo (SALDANHA, 2000).

Conforme os conceitos acima citados, a análise de impacto é um procedimento de extrema importância e o passo inicial quando o objetivo final é segurança.

Nesta etapa serão identificados os processos essenciais para a continuidade dos negócios de uma organização. Para isso, um cenário fictício deverá ser apresentado com a finalidade de representar um desastre significativo. À medida que a apresentação do cenário for sendo feita, surgirão os processos que não poderão sofrer paralisações. Esses processos precisam ser analisados e classificados por ordem de importância para a sobrevivência da organização.

O cenário fictício que será apresentado deve ser o mesmo para toda a organização, a fim de que o grau de criticidade usado na análise de impacto tenha a mesma proporção. O procedimento para Análise de Impacto deverá se repetir o número de vezes correspondente ao de unidades da organização, porém em unidades separadas. A individualidade do procedimento possibilitará uma visão geral da organização, além de proporcionar um levantamento das atividades individuais de cada funcionário.

Dessa maneira, a segurança e o comprometimento com a continuidade do negócio passarão a ser responsabilidades de todos os envolvidos no negócio.

Após obtidos os processos considerados essenciais para a organização, esta deverá explicitar os pontos que considera de maior valor, ou seja, apresentar suas maiores preocupações (SALDANHA, 2000).

A organização em questão deve considerar quatro impactos dos abaixo apresentados. Por exemplo, determinada organização pode ter as seguintes preocupações:

- preservação da segurança do pessoal.
- preservação da confiança de acionistas.
- preservação de vantagens competitivas.
- preservação da empresa diante de perdas financeiras para a organização.
- preservação da satisfação do cliente.
- preservação da imagem.
- preservação da empresa diante de danos de ordem pública. Os valores selecionados passarão a formar um conjunto representativo da cultura da organização (SALDANHA, 2000).

Esta metodologia propõe o uso de 4 impactos por se tratar de uma metodologia simplificada, elaborada com o objetivo de auxiliar empresas de pequeno porte. O uso desta metodologia em empresas de portes maiores poderá implicar no uso de todos os impactos mencionados ou até mesmo na adição de novos impactos considerados importantes para a empresa em questão.

O próximo passo é a adição de pesos ou de graus de importância para cada uma das preocupações classificadas anteriormente.

3.4 Inserção de Valores aos Impactos Classificados

As organizações têm diferentes focos no que diz respeito à segurança. Algumas dão importância com maior intensidade para as perdas financeiras, enquanto para outras o mais importante é preservar a credibilidade. Em razão disso serão utilizados valores que representarão graus de importância. Por exemplo, a organização que visa a preservar o atendimento a seus clientes atribuirá um valor alto e coerente com a importância. Assim, os

graus de importância para os impactos mudarão conforme a organização onde a metodologia esteja sendo aplicada. O grupo de trabalho responsável por essa tarefa terá a flexibilidade na atribuição de valores conforme o grau de importância de determinados impactos. Por exemplo, uma empresa que define suas preocupações como a perda de credibilidade, satisfação do cliente, perda financeira e preservação da confiança de acionistas deverá atribuir a essas preocupações valores diferentes. Os mais altos são adicionados para as maiores preocupações e os valores menores, para as menores preocupações.

Para exemplificar serão atribuídos valores de 1 a 4 para os impactos citados acima:

Impacto	**Valores**
Perda de Credibilidade	2
Satisfação do Cliente	2
Perda Financeira	4
Confiança dos acionistas	3

Após classificadas as prioridades, o próximo passo é representar, por meio de fluxograma, os processos considerados críticos.

3.5 Apresentação dos Processos de Cada Unidade

Os processos destacados como os mais importantes para a organização deverão ser apresentados de forma ilustrativa. É preciso mostrar os processos dos quais ele depende e/ou aqueles que dependem dele.

A organização deverá representar esses processos usando diferentes modelos de fluxograma adequado aos diferentes tipos de processos realizados pela mesma.

3.6 Análise de Riscos

Nesta etapa, o grupo de trabalho responsável pelos processos realizados na organização responderá um questionário. Este resultará em um diagnóstico da situação atual da organização e apontará suas vulnerabilidades, permitindo a escolha da melhor opção para a resolução dos problemas momentâneos.

Segundo Saldanha (2000), esta etapa considera quatro variáveis: perdas possíveis, ameaças, vulnerabilidades e controles.

De acordo com Ferreira (1993):

> Ameaça: “ ...Prenúncio ou indício de coisa desagradável ou temível, de desgraça,...”
>
> Vulnerável: “Lado fraco de um assunto, ou de uma questão, ou do ponto pelo qual alguém pode ser atacado ou ferido.”
>
> Desastre: “Acontecimento calamitoso, especialmente o que ocorre de súbito e ocasionando grande dano ou prejuízo.”
>
> Risco: “ Possibilidade de perda ou de responsabilidade pelo dano.”

As definição feitas por Saldanha (2000) são:

- **Ameaça** é toda e qualquer condição adversa, capaz de vir a causar alguma perda para a empresa.
- **Vulnerabilidade** é um item que aumenta a exposição a um desastre, por tornar a concretização deste mais provável.
- **Desastre** é o impacto de uma força externa agressiva (ameaça), ocasionando perda ou prejuízo significativo.
- **Risco** é uma medida numérica ou relativa, que quantifica ou qualifica a probabilidade da ocorrência do desastre.

Conforme a norma ISO 17799, a análise de risco é um processo de avaliação dos riscos, observando quais são os pontos vulneráveis de uma organização. Baseada nesses resultados, a organização deverá avaliar a probabilidade de ocorrência de possíveis incidentes devido às vulnerabilidades observadas.

A seguir é apresentado um questionário simplificado, que tem por base o conjunto de perguntas propostas por Saldanha (2000). O seu uso visa demostrar as vulnerabilidades da organização e justificar o acréscimo de medidas preventivas.

Os tópicos abordados são:

1 – Instalações.

2 – Pessoal.

3 - Instituições operacionais.

4 - Controle de acesso físico.

5 - Controle de acesso lógico.

6 - *Back-up* de arquivos.

7 – Seguro.

TÓPICO	ASSUNTO	QUESTÕES
Instalações	Exposição a fogo	- Existe equipamento de combate a incêndio? - Os equipamentos de combate a incêndio são mantidos carregados e em condições de uso? - Os equipamentos de detecção de fogo são regularmente testados?
	Ar condicionado	- Existe sistema de ar condicionado exclusivo para a área onde estão os servidores?
	Parte elétrica	- A fonte de energia local é confiável e estável? - A tensão e a amperagem é suficiente para a operação simultânea de todos os aparelhos? - O suprimento de energia é suscetível a: - Picos? - Baixa de tensão? - Queda de energia? - Existem geradores de energia? - Existem *no-breaks*? - A tensão de entrada é monitorada por um voltímetro que mantém os dados registrados? - O sistema elétrico está devidamente aterrado? - A empresa possui conexão estável com a Internet 24 horas por dia os 7 dias da semana?

TÓPICO	ASSUNTO	QUESTÕES
Pessoal	Procedimentos e Treinamento	- Na contratação de novos funcionários, é feita uma checagem do seu histórico profissional? - Os funcionários são avisados quanto ao seu comprometimento com a política de segurança da organização e suas devidas punições?
		- O pessoal é treinado quanto ao desligamento ou não das máquinas e quanto aos procedimentos normais de segurança? - Existe um programa de conscientização da importância da segurança? - Os funcionários têm conhecimento dos locais onde estão os equipamentos de reserva e os dispositivos contendo os arquivos de *back-up*?
	Instruções Operacionais	- O pessoal é instruído quanto aos procedimentos de: - Uso de extintores? - Telefones de emergência? - Polícia? - Ambulância? - Primeiros Socorros?
Segurança dos equipamentos	Controle de Acesso Físico	- As áreas vitais da organização são protegidas com controle de acesso físico? - Em caso de serviços terceirizados, os funcionários que executarão os serviços assinam algum tipo de documento se comprometendo com a Segurança? - Existe algum dispositivo de controle de acesso com mecanismo de alerta em caso de tentativa de acesso não autorizado? - Em caso de demissão, as tabelas de controle de acesso são atualizadas imediatamente? - O prédio possui guardas controlando entrada e saída de equipamentos 24 horas por dia 7 dias na semana?

TÓPICO	ASSUNTO	QUESTÕES
Segurança dos equipamentos	Controle de Acesso Físico	- O prédio possui câmaras para controle de acesso? - Existe cadastro para controlar a entrada e saída do prédio? - As máquinas possuem tranca para evitar roubos internos?
	Controle de Acesso Lógico	- Existe algum tipo de dispositivo do tipo "*Firewall*" para proteger acessos não autorizados? - Existe algum dispositivo de alerta em caso de acesso não autorizado? - Os micros integrados à LAN (Local Area Network) possuem *modems* de acessos a linhas externas? - É mantido o *log* dos acessos aos arquivos e bancos de dados críticos? - Existe uma rotina que emita relatórios diários de tentativas de acesso? - No caso de demissão de funcionários, suas senhas de acesso são eliminadas com urgência? - Existe registro dos equipamentos contidos na organização (data da compra, instalação, manutenções realizadas, problemas detectados, etc.)? - Existem equipamentos reserva, caso aconteçam falhas inesperadas nos que estão sendo utilizados? - Esses equipamentos reserva são testados periodicamente? - Esses equipamentos suportam o processamento dos procedimentos realizados na organização? - Os equipamentos reserva estão em prédios separados? - Esses equipamentos são de fácil acesso?

TÓPICO	ASSUNTO	QUESTÕES
Segurança dos equipamentos	Segurança dos Arquivos	- São feitos *back-ups* periódicos de arquivos críticos? - A periodicidade em que os *back-ups* são feitos atende a demanda de informações? - Os dispositivos contendo os *back-up* são arquivados em locais de fácil acesso? - Esses dispositivos são guardados remotamente? - A empresa possui espelhamento e sincronização de seus dados cruciais? - Os equipamentos usados para o espelhamento estão localizados em prédio distintos? - A empresa possui rotinas para verificação da integridade dos dados do seu site?
	Seguro	- A organização possui seguro? - O seguro é coerente com as necessidades da organização? - As cláusulas desse seguro são revistas periodicamente, conforme mudanças ocorridas na organização?

As respostas obtidas terão uma ligação com os impactos já classificados anteriormente e com seus devidos valores atribuídos. Os resultados (valores) dessa ligação passarão por uma somatória em que serão demonstradas as criticidades e a urgência de adição de procedimentos de segurança. Assim, aquelas respostas negativas que influenciarão em impactos com maiores valores deverão ter uma atenção especial em relação às outras, e precisam ser adicionados procedimentos imediatos que previnam acidentes decorrentes dessas vulnerabilidades.

Para a melhor visualização, os resultados deverão ser apresentados em gráficos, a serem elaborados na etapa Resultado da Análise.

3.7 Resultado Final

Esta etapa apresenta os resultados obtidos após a aplicação da metodologia, possibilitando que a empresa analisada tome conhecimento de seu estado de segurança. Os resultados poderão ser representados através de gráficos, para facilitar a visualização do diagnóstico realizado. Para a elaboração dos gráficos poderá ser usado um esquema de pontuação atribuído pela própria empresa.

Um ponto relevante e positivo da metodologia proposta é a flexibilidade de adequação dos requisitos de segurança que são testados e dos impactos que são considerados para geração dos resultados. A empresa que utilizar a metodologia terá liberdade de adequação dos seguintes requisitos propostos neste trabalho:

- A quantidade de impactos e quais impactos serão utilizados para gerar os resultados poderão ser selecionados conforme a necessidade da empresa, além da possibilidade de adicionar novos impactos, de forma a constituírem a cultura organizacional da empresa em questão.
- Na etapa de inserção de valores aos impactos selecionados, o grupo de trabalho que possui esta incumbência poderá optar por um range de pontuação adequado para representar a criticidade dos itens a serem avaliados.

- A empresa poderá adicionar, excluir ou detalhar os quesitos do questionário proposto pela M.A.S na etapa de Análise de Risco.

Este trabalho aplica a metodologia em uma empresa que tem como ramo de atividade a emissão de certificados digitais e necessita de segurança para proteger toda sua estrutura. O item seguinte apresenta o resultado desta aplicação.

3.7.1 Resultado da Aplicação da M.A.S em uma ICP

Esta etapa apresenta os resultados obtidos após a aplicação da metodologia em uma Infra-estrutura de Chave Pública que será representada pela denominação XYZ.

Conforme a seqüência proposta pela metodologia, a primeira etapa é a Análise de Impacto. Para a realização desta etapa, utilizou-se uma situação fictícia para simular o acontecimento de um desastre. A situação foi a ocorrência de um incêndio, em que as informações seriam perdidas, os clientes deixariam de ser atendidos, a segurança das pessoas que trabalham na empresa bem como a imagem desta ficariam comprometidas. A partir da simulação foram levantados os processos que não podem sofrer paralisações. No caso da empresa XYZ, os seguintes processos foram considerados vitais e fazem parte da mesma unidade de serviço:

- Módulo Público: processo responsável em fornecer acesso ao público para a realização de pedidos de certificados digitais através da Internet.
- Autoridade de Registro: processo responsável em executar a conferência dos dados contidos nos pedidos de certificados digitais.
- Autoridade Certificadora: processo responsável em emitir certificados digitais mediante certificação da conferência dos dados do pedido.

A Figura 10 ilustra o funcionamento desses processos e suas dependências.

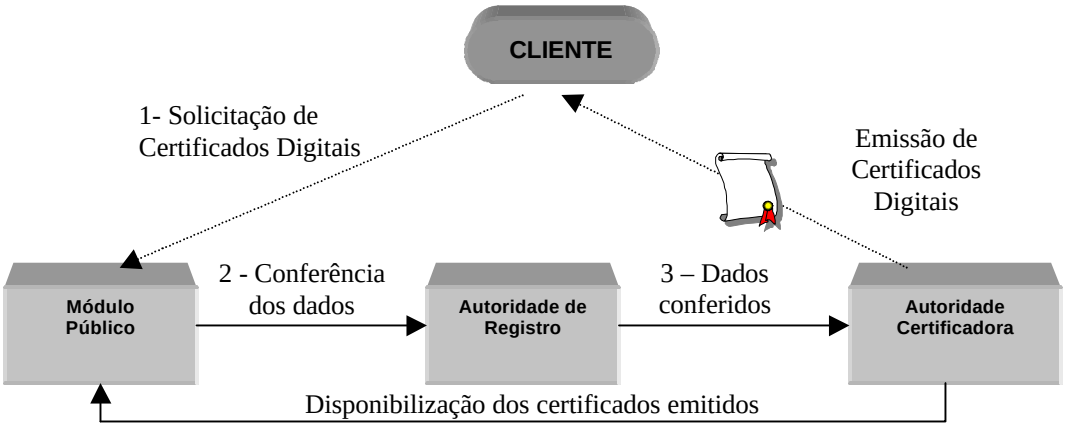


Figura 10 – Fluxograma dos processos

O próximo passo realizado foi a atribuição de valores aos impactos, demostrando quais são as maiores preocupações da empresa XYZ. Foram convencionados valores de 1 a 4. Os números maiores representavam as maiores preocupações; os números menores, as preocupações menos relevantes.

Conforme a cultura da empresa XYZ, a tabela de impactos foi preenchida com os seguintes valores:

Impacto	Peso
Atendimento ao cliente	3
Perdas Financeiras	2
Segurança do Pessoal	4
Imagem da empresa	3

A tabela mostra que a maior preocupação da empresa é com a segurança do pessoal. Em segundo lugar estão o atendimento ao cliente e a sua imagem. Por último, está a preocupação com perdas financeiras.

Para classificar os impactos e as perguntas contidas no questionário conforme a ordem de importância, foi utilizada uma pontuação entre 1 e 4. A pontuação utilizou esta faixa de números devido ao fato de que a metodologia foi aplicada em uma ICP de pequeno porte e sua aplicação neste trabalho, tem como objetivo principal testar a metodologia e não diagnosticar a empresa XYZ. Dessa forma, a faixa de números utilizada atende os objetivos. Essa pontuação poderia utilizar um intervalo maior de números conforme a necessidade de representar as diferentes importâncias ente os requisitos que serão avaliados.

Na etapa seguinte, denominada Análise de Risco, o questionário foi respondido, tornando possível a criação dos gráficos e a geração de uma pontuação utilizada para, na seqüência, classificar as questões.

Para gerar a pontuação, convencionou-se que cada pergunta receberia um valor entre 0 e 4 (valores pré-definidos), e que a mesma influenciaria em, no máximo, dois impactos. Combinando as respostas do questionário com os valores atribuídos à tabela de impactos, as questões foram classificadas conforme a pontuação alcançada.

Com base nesta convenção, as perguntas utilizaram um range entre 1 e 4 e os níveis de classificação foram: Sem problemas, Nível 1, Nível 2 e Nível 3, sendo:

- Sem Problemas (não apresenta problemas de segurança): A questão recebe esta classificação quando a pontuação alcançada for igual a 0, ou seja, o requisito de segurança já existe.
- Nível 1 (são problemas que devem ser tratados, porém não com urgência): A questão recebe esta classificação quando a pontuação alcançada for igual ou inferior a 10 pontos.
- Nível 2 (são problemas que devem ser tratados com urgência): A questão recebe esta classificação quando a pontuação alcançada permanece entre 11 e 31 pontos.
- Nível 3 (são problemas graves, que devem ser tratados imediatamente): A questão recebe esta classificação quando a pontuação alcançada for igual a 32 pontos.

Esses valores foram criados a partir dos seguintes pressupostos:

- Cada questão influenciará no máximo em dois impactos, conforme notificado anteriormente.
- O maior peso permitido para os impactos é 4.
- As perguntas recebem valores entre 0 e 4, conforme o grau de importância de seu conteúdo.

Considerando: a variável X para representar o valor dado a questão; Y1 para representar o valor atribuído a um dos impactos relacionados com a pergunta; e Y2 para representar o valor concebido ao outro impacto relacionado com a pergunta, podemos utilizar a seguinte fórmula:

$$(X * Y1) + (X * Y2)$$

Sendo assim, a avaliação de uma questão com valor 4, que influencie nos aspectos considerados de extrema importância pela empresa (ambas com valor 4), terá um resultado igual a 32.

$$(4 * 4) + (4 * 4) = 32$$

Portanto, questões que retratem péssimas condições, ou seja, aquelas respostas que influenciam negativamente nos objetivos da empresa, terão no máximo a pontuação 32. Considerando este valor como a pontuação máxima possível, ou seja, como questão de Nível 3, conclui-se que a empresa deverá atendê-las com urgência.

Em relação às pontuações do Nível 1 e Nível 2, foram utilizadas frações decimais para a definição das faixas de pontos.

Conforme apresentado anteriormente, o quadro de impactos da empresa XYZ foi preenchido com os seguintes pesos:

Impacto	**Peso**
Atendimento ao cliente	3
Perdas Financeiras	2
Segurança do Pessoal	4
Imagem da empresa	3

Utilizando os valores da tabela de impacto e as respostas obtidas do questionário, foram gerados os seguintes gráficos apresentados nas Figuras 11 e 12:

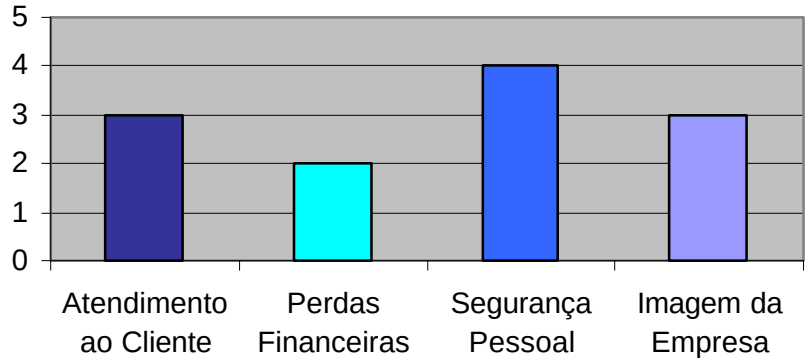


Figura 11 – Preocupação da empresa

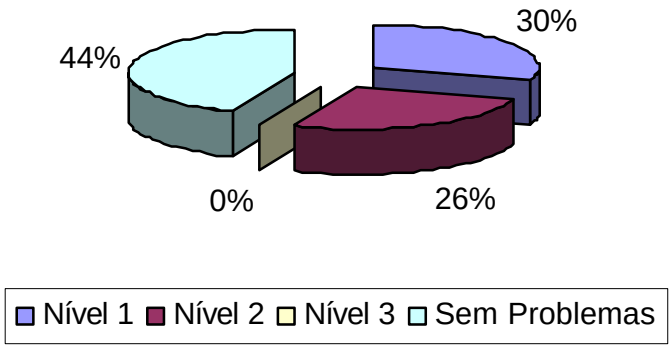


Figura 12 – Resultados em níveis

Considerando os pesos atribuídos às preocupações da empresa, o percentual das questões classificadas como Nível 3 foi de 0%; como Nível 2 foi de 26%; e como Nível 1 foi de 30%. Os cálculos utilizados para apresentar os resultados mostraram que a empresa XYZ não possui vulnerabilidade que comprometa criticamente seus objetivos, pois nenhuma questão recebeu a pontuação máxima.

O uso de porcentagem para representar os resultados foi adotado para facilitar sua visualização, pois, não significa que uma empresa que apresente 0% de questões classificadas como Nível 3 e 80% de questões classificadas como Nível 1 não necessite de procedimentos de segurança. Uma empresa que apresente 80% das questões classificadas como Nível 1 (problemas que devem ser tratados, porém não com urgência) não poderá ignorar o tratamento

das questões. Estes problemas poderão, em um curto espaço de tempo, e devido a alta porcentagem, ter sua classificação alterada, podendo até acarretar problemas de Nível 3. Esta metodologia não menciona o crescimento do problema, pois utiliza a classificação dos problemas em níveis somente para auxiliar na ordem de prioridade de inserção dos procedimentos de segurança, considerando que todos os níveis, exceto o Nível 0, receba o tratamento necessário.

Este método utilizado para apresentar os resultados da M.A.S. tem o objetivo de simplificar o processo de criação dos gráficos. Porém, poderão ser utilizados outros cálculos e outros métodos para visualizar os resultados desta metodologia.

Após os resultados verdadeiros da análise, foram feitas algumas alterações nos pesos atribuídos às preocupações, ou seja, na tabela de impactos. Verificou-se que os resultados finais sofreram grandes mudanças. Isso ocorreu devido ao fato de que esta metodologia foi desenvolvida levando em conta a cultura como um fator relevante para o resultado da análise e de que as necessidades das empresas são diferentes.

No gráfico a seguir pode-se observar o resultado da análise após as alterações. Para a geração deste gráfico, foi considerado o questionário contendo as mesmas respostas. As alterações foram feitas somente na tabela de preocupações. Porém, o resultado apresentou uma grande alteração na necessidade de contingenciamento imediato da empresa.

Impacto	**Peso**
Atendimento ao cliente	4
Perdas Financeiras	4
Segurança do Pessoal	2
Imagem da empresa	3

Os resultados obtidos a partir da tabela modificada foram apresentados nas Figuras 13 e 14.

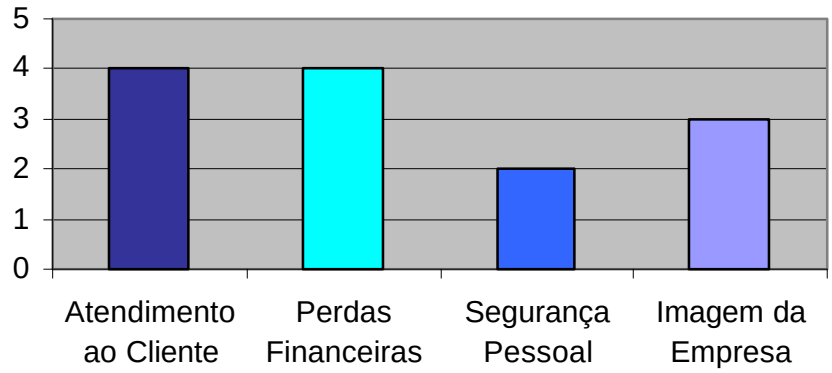


Figura 13 – Preocupação da empresa a partir da tabela modificada

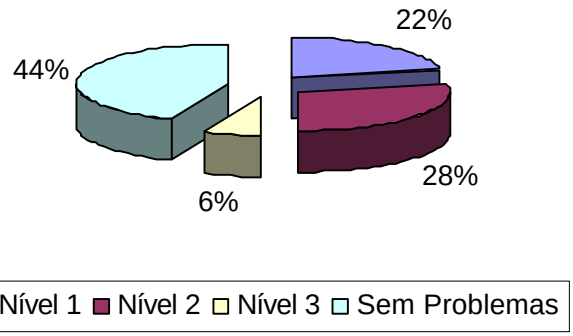


Figura 14 – Resultados em níveis a partir da tabela modificada

Neste exemplo, a segurança da empresa apresenta problemas mais graves, pois o percentual das questões classificadas como Nível 3 foi de 6%; como Nível 2 foi de 28%; e como Nível 1 foi de 22%. Houve um aumento significativo no percentual das questões vulneráveis, principalmente as de Nível 3. Isso significa que a maioria das falhas de segurança está nas questões que prejudicam diretamente os objetivos da empresa.

Os problemas detectados com a aplicação da metodologia podem ser solucionados com técnicas que auxiliam na definição da prioridade de contingenciamento baseando-se em custos. Um exemplo é o BIA *(Business Impact Analisys*). Esta técnica avalia, a partir dos processos críticos e vitais da empresa, quais os valores que esses processos envolvem direta ou indiretamente o negócio. Assim, define a ordem do contingenciamento e os investimentos necessários à sua manutenção após a ocorrência de um possível desastre.

Essas técnicas terão maior contribuição para empresas que apresentam uma quantidade grande de questões críticas, ou seja, grande quantidade de questões que necessitam

de providências imediatas. Dessa forma, as técnicas auxiliarão a decidir a ordem do contingenciamento, considerando os custos.

CAPÍTULO IV
CONSIDERAÇÕES FINAIS E SUGESTÕES

4.1 Considerações Finais

O presente trabalho apresentou a Metodologia Simplificada para Análise de Segurança - M.A.S., aplicada em uma empresa cujo negócio é Infra-estrutura de Chave Pública (ICP). A M.A.S. foi desenvolvida para possibilitar que essas empresas tenham conhecimento e saibam exatamente quais os aspectos de segurança que deverão ser tratados com prioridade.

A segurança da informação não é um produto, e sim um processo. É uma combinação de equipamentos seguros e práticas seguras. É extremamente importante para um empresa do tipo ICP estar segura, pois antes de fornecer segurança é necessário cercar-se dela.

Por ser flexível e possibilitar alterações em seu conteúdo, esta metodologia pode ser remodelada e aplicada em empresas que executam outras atividades. Embora existam inúmeros *check-lists* desenvolvidos com a finalidade de avaliar níveis de segurança, cada empresa tem características e necessidades próprias. Por esse motivo, além da lista de aspectos básicos de segurança, a M.A.S. apresenta os itens específicos a serem avaliados em um trabalho de diagnóstico da ICP, onde a metodologia foi aplicada. A M.A.S. considera também, para geração do resultado, a cultura organizacional da empresa em que está sendo aplicada.

Com a M.A.S. os objetivos deste trabalho foram alcançados. Sua simplicidade e flexibilidade contribuem para que empresas como as ICPs identifiquem suas vulnerabilidades e minimizem as fontes de riscos.

A definição de uma M.A.S. para uma ICP pode ser o primeiro passo de um grande processo a ser realizado para garantir a segurança das informações. Dessa forma, os estudos

não deverão ser encerrados por aqui, e sim devem servir como ponto de partida para novos trabalhos.

4.2 Sugestões para Trabalhos Futuros

Outros trabalhos poderão se desenvolver a partir da metodologia proposta nesta dissertação. As sugestões para trabalhos futuros são:

- Desenvolvimento de uma aplicação para auxiliar no tratamento dos problemas de segurança diagnosticados pela M.A.S. Deverão ser realizados estudos das soluções de segurança, suas vantagens e desvantagens, seus respectivos custos e estes, armazenados em um banco de dados de forma que cada problema tenha uma série de soluções disponíveis para resolvê-los.
- Estudo de redes neurais contribuindo para a melhoria da elaboração de uma metodologia similar a que foi proposta neste trabalho utilizando redes neurais.
- Estudo da lógica fuzzy para a elaboração de uma metodologia similar a que foi proposta neste trabalho, de forma que, o questionário possa ser respondido não somente com respostas binárias, mas também com respostas intermediárias entre Sim e Não.
- Estudo de formas de aplicação da norma ISO 17799, podendo esta ser utilizada para análise, para implementação da segurança ou para certificação. Este trabalho poderia propor as maneiras que a norma poderá ser utilizada para contribuir com a segurança de uma empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAMS, C.; LLOYD, S. **Understanding Public-Key Infrastructure:** Concepts, Standards, and DeplymentConsiderations. [S.l.]: Macmillan Technical Publishing, 1999.

ALEVATE, W. **Conheça o PCN e descubra o que ele pode fazer por sua empresa**. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em : 10 dez. 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação**: código de prática para gestão da segurança da informação – NBR ISO/IEC 17799. Rio de Janeiro, 2001.

BEAL, A .**Manual de Planejamento da Continuidade do Negócio.** Brasília: Vydia Tecnologia, 2001.

CERTISIGN. Empresa brasileira atuando como autoridade certificadora. Disponível em: <http://www.certisign.com.br>. Acesso em: 10 dez. 2001.

FEGHHI, J. F.; WILLIAMS, P. **Digital Certificates**. [S.l.]: Addison Wesley, 1999.

GARFINKEL, S.; SPAFFORD, G. **Comércio & Segurança na Web :** riscos, tecnologias e estrategias. São Paulo: Makron Books, 1999.

HOUSLEY, Russ; POLK, Tim. **Planning for PKI**: Best Practices Guide for Deploying Public Key Infrastructure. USA: John Wiley & Sons, 1999

IBM. **Continuidade dos negócios:** novos riscos, novos imperativos e uma nova abordagem. 2001. Disponível em http://www-5ibm.com/pt/services/its/bcrs/gsopa40.pdf acessado em 28/11/2001.

INTERSIX. Empresa integradora de soluções formada por um grupo de profissionais brasileiros especializados em Tecnologia da Informação, redes e desenvolvimento de software. Disponível em: <http://www.intersix.com.br>. Acesso em: 12 dez. 2001.

MAIA, M.A. **A Política de Segurança garantindo a continuidade do negócio.** Disponível em: <http://www.modulo.com.br>. Acessado em: 13/11/2001.

MARINHO, Fernando. Saiba o que é PCN. Disponível em: < http://www. teleoffice.com.br/pcn.htm >. Acessado em: 13/11/2001.

SALDANHA, F. **Introdução a Planos de Continuidade e Contingência Operacional**. Rio de Janeiro: Papel Virtual, 2000.

SALDANHA, F. **Entendendo um Plano de Continuidade de Negócios**. Disponível em: <http://www.securenet.com.br/artigo.php?artigo=22>. Acesso em: 13 nov. 2001.

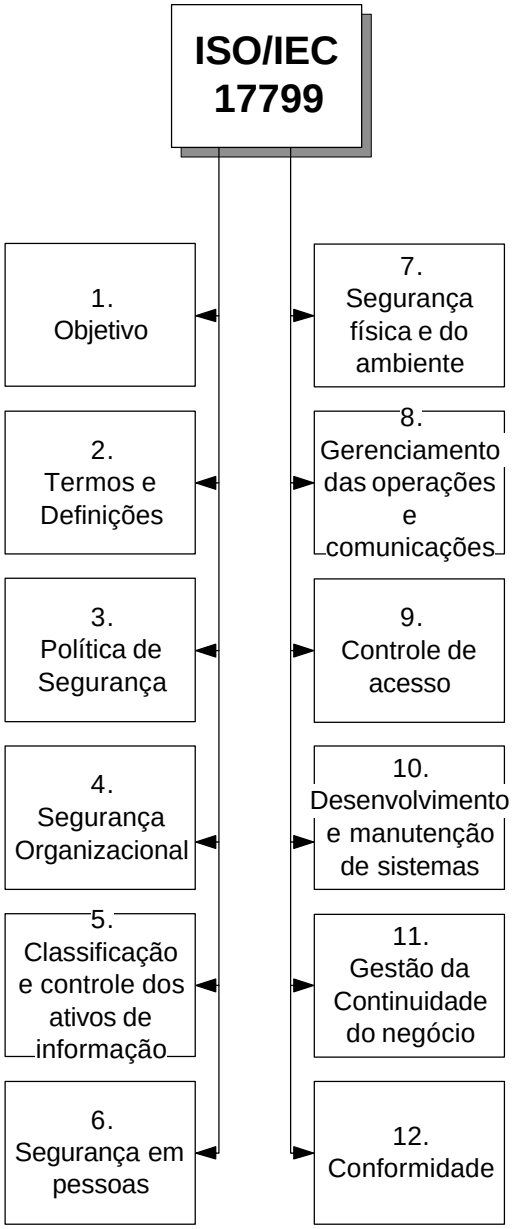
STALLINGS, W. **Cryptography and Network Security –Principles and Practic**e. 2. ed. [S.l.]: Prentice-Hall, 1999.

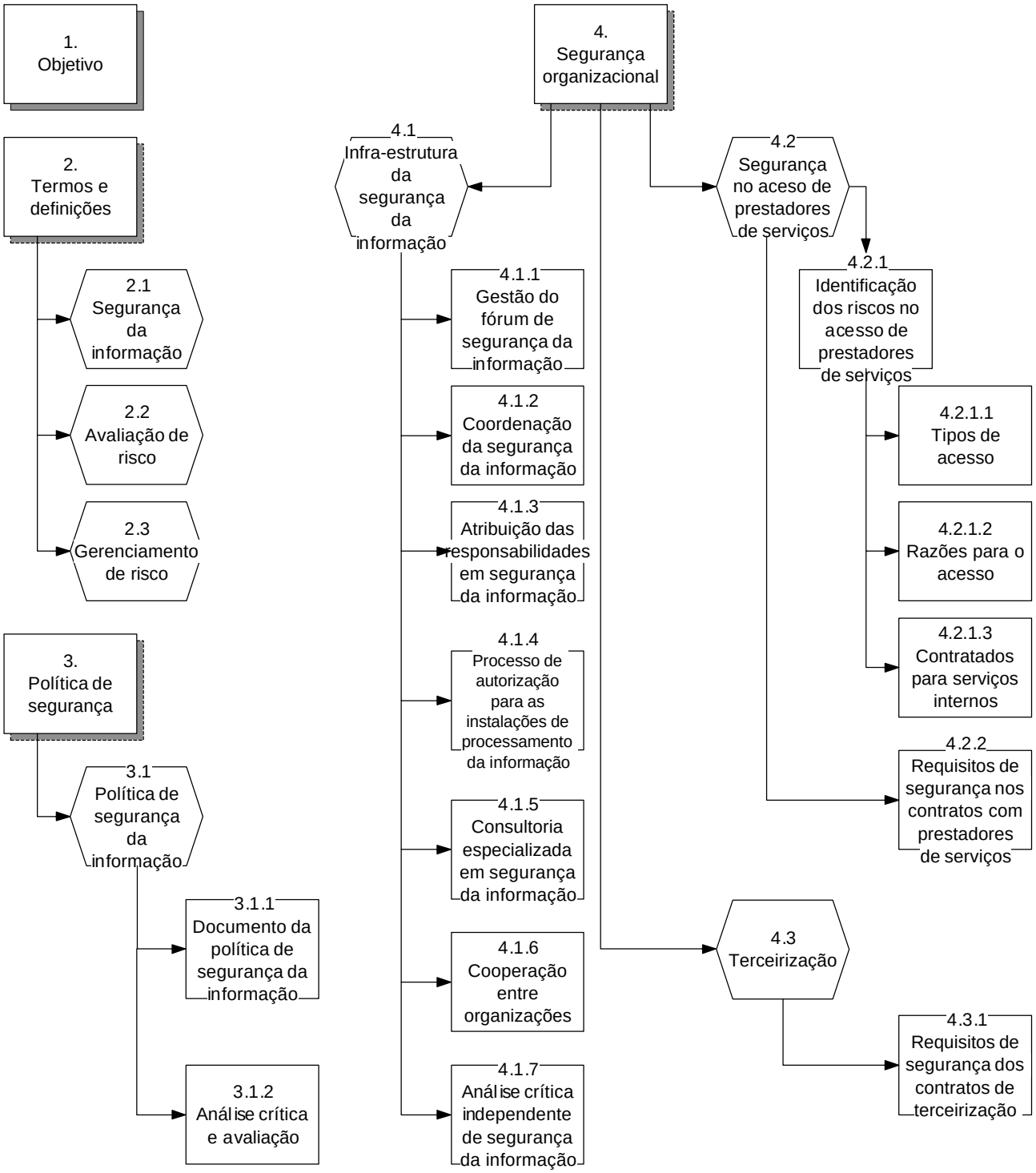
STINSON, D. R. **Cryptography** : theory and practice. [S.l.]: CRC Press LLC, 1995.

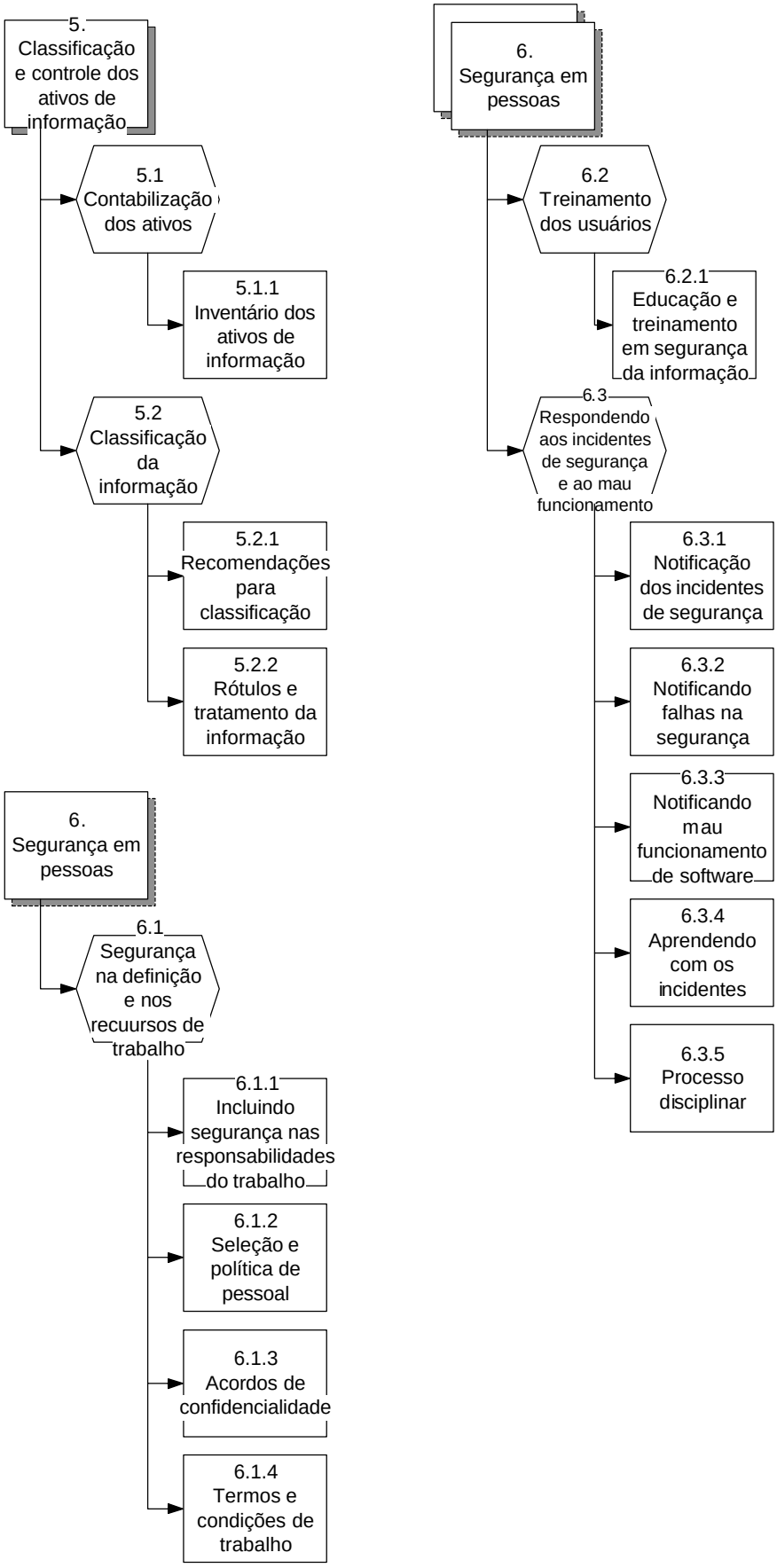
UNION, I. T. ITU-T recommendation x.509. Junho 1997.

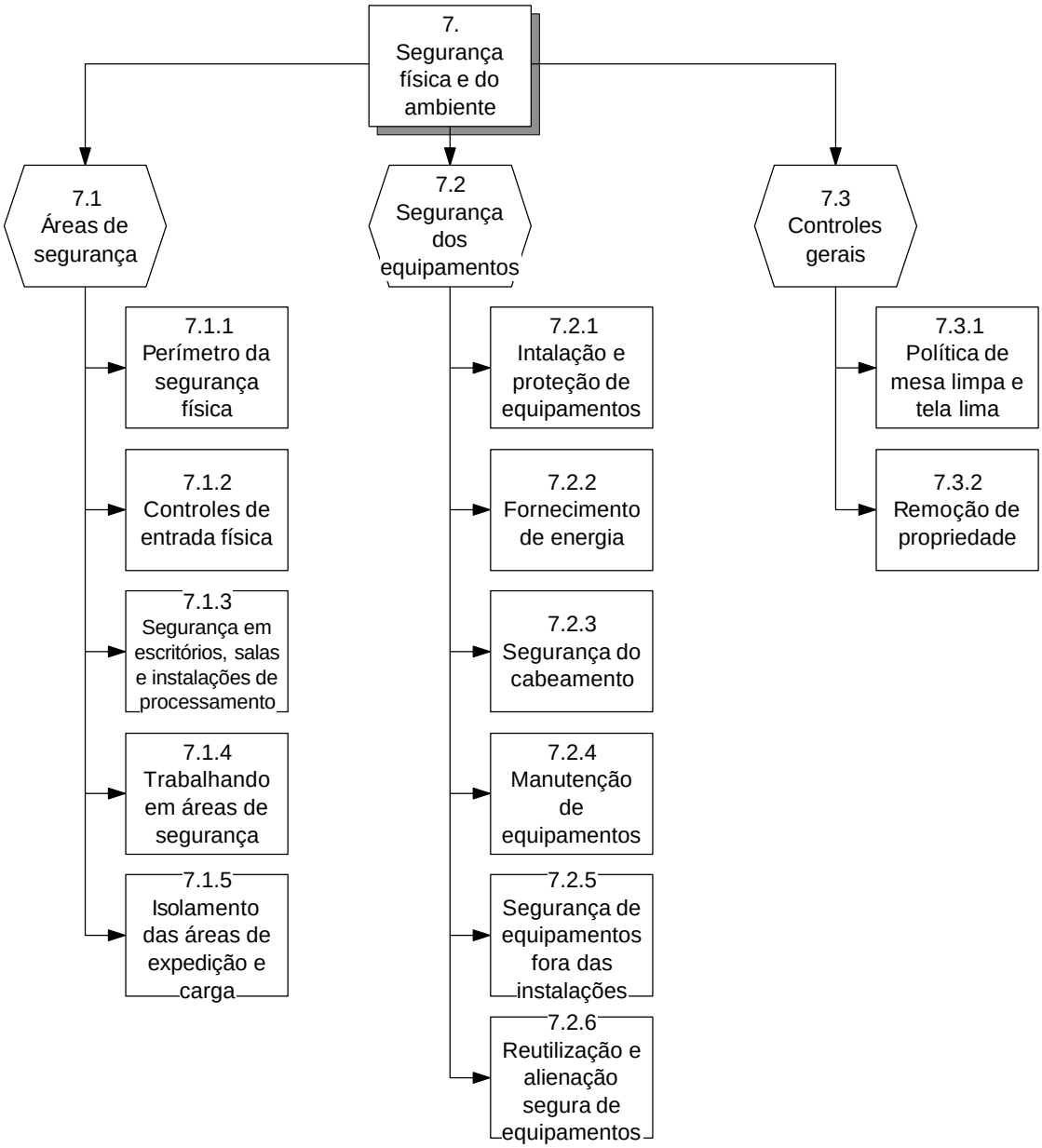
ANEXOS

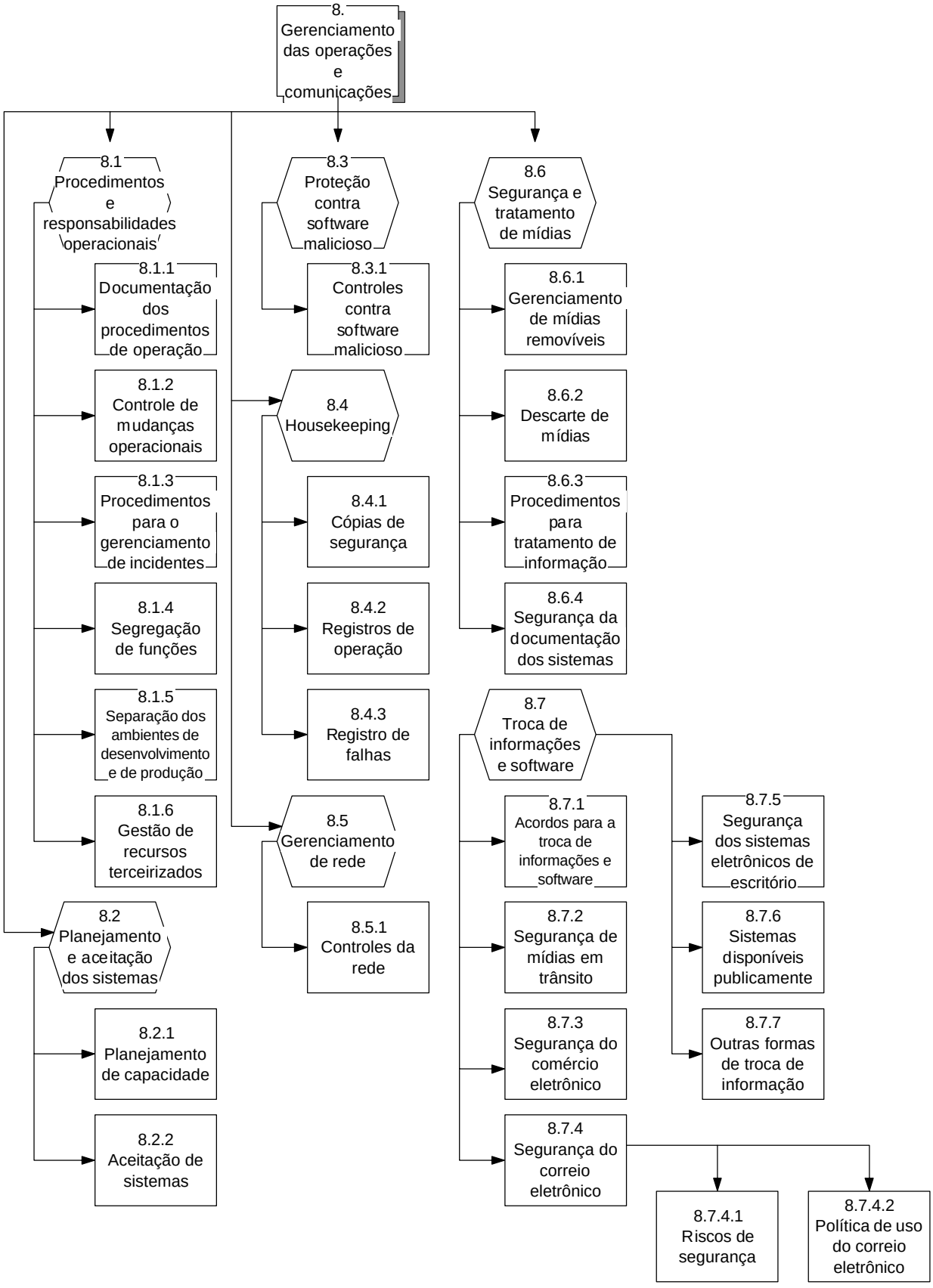
ANEXO A - Representação Gráfica da Norma ISO 17799

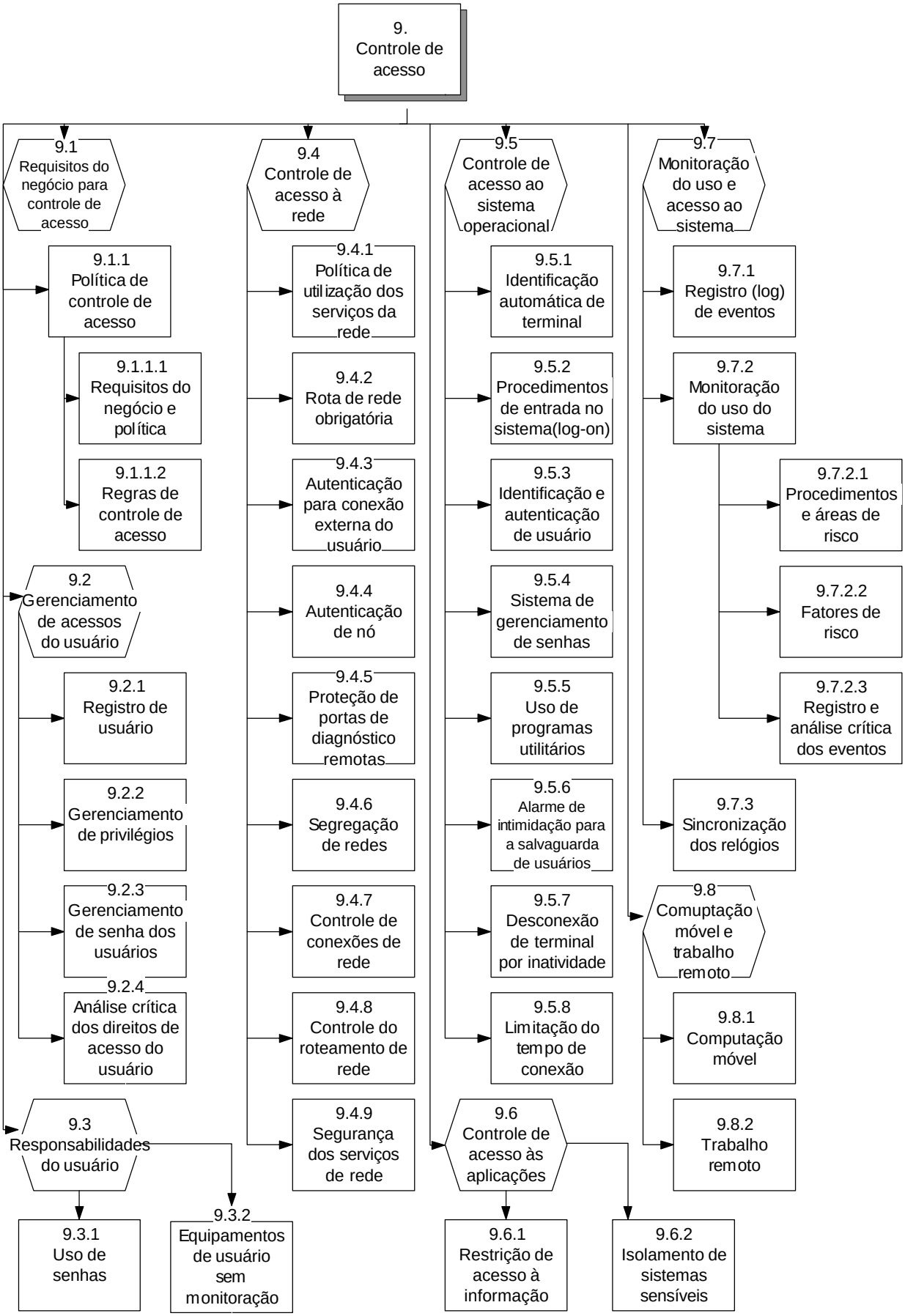


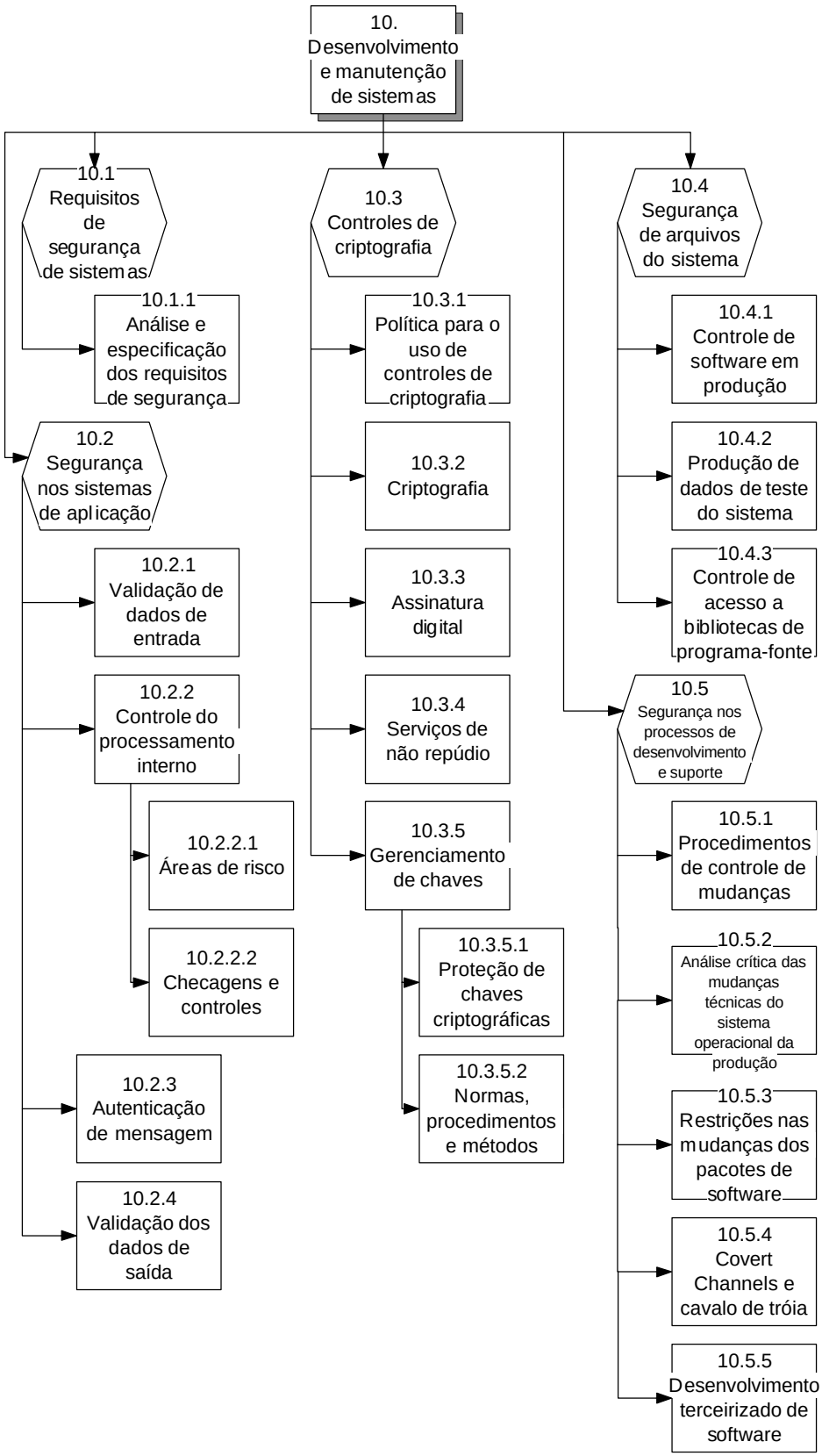

1.
Objetivo
2.
Termos e definições
2.1
Segurança da informação
2.2
Avaliação de risco
2.3
Gerenciamento de risco
3.
Política de segurança
3.1
Política de segurança da informação
3.1.1
Documento da política de segurança da informação
3.1.2
Análise crítica e avaliação
4.
Segurança organizacional
4.1
Infra-estrutura da segurança da informação
4.1.1
Gestão do fórum de segurança da informação
4.1.2
Coordenação da segurança da informação
4.1.3
Atribuição das responsabilidades em segurança da informação
4.1.4
Processo de autorização para as instalações de processamento da informação
4.1.5
Consultoria especializada em segurança da informação
4.1.6
Cooperação entre organizações
4.1.7
Análise crítica independente de segurança da informação
4.2
Segurança no aceso de prestadores de serviços
4.2.1
Identificação dos riscos no acesso de prestadores de serviços
4.2.1.1
Tipos de acesso
4.2.1.2
Razões para o acesso
4.2.1.3
Contratados para serviços internos
4.2.2
Requisitos de segurança nos contratos com prestadores de serviços
4.3
Terceirização
4.3.1
Requisitos de segurança dos contratos de terceirização

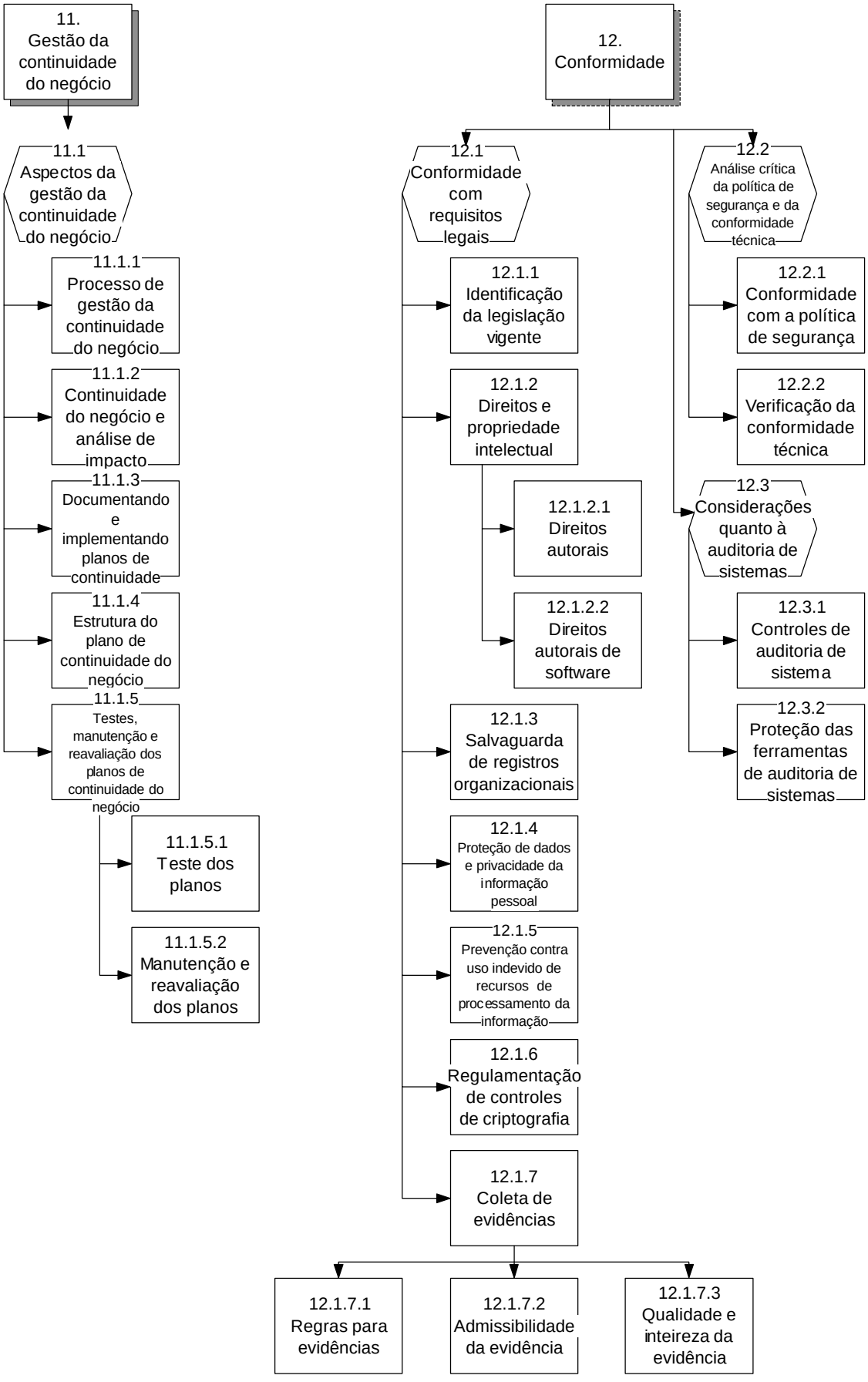

5. Classificação e controle dos ativos de informação
5.1 Contabilização dos ativos
5.1.1 Inventário dos ativos de informação
5.2 Classificação da informação
5.2.1 Recomendações para classificação
5.2.2 Rótulos e tratamento da informação
6. Segurança em pessoas
6.1 Segurança na definição e nos recuursos de trabalho
6.1.1 Incluindo segurança nas responsabilidades do trabalho
6.1.2 Seleção e política de pessoal
6.1.3 Acordos de confidencialidade
6.1.4 Termos e condições de trabalho
6. Segurança em pessoas
6.2 Treinamento dos usuários
6.2.1 Educação e treinamento em segurança da informação
6.3 Respondendo aos incidentes de segurança e ao mau funcionamento
6.3.1 Notificação dos incidentes de segurança
6.3.2 Notificando falhas na segurança
6.3.3 Notificando mau funcionamento de software
6.3.4 Aprendendo com os incidentes
6.3.5 Processo disciplinar


7. Segurança física e do ambiente
7.1 Áreas de segurança
7.2 Segurança dos equipamentos
7.3 Controles gerais
7.1.1 Perímetro da segurança física
7.1.2 Controles de entrada física
7.1.3 Segurança em escritórios, salas e instalações de processamento
7.1.4 Trabalhando em áreas de segurança
7.1.5 Isolamento das áreas de expedição e carga
7.2.1 Intalação e proteção de equipamentos
7.2.2 Fornecimento de energia
7.2.3 Segurança do cabeamento
7.2.4 Manutenção de equipamentos
7.2.5 Segurança de equipamentos fora das instalações
7.2.6 Reutilização e alienação segura de equipamentos
7.3.1 Política de mesa limpa e tela lima
7.3.2 Remoção de propriedade


8. Gerenciamento das operações e comunicações
8.1 Procedimentos e responsabilidades operacionais
8.1.1 Documentação dos procedimentos de operação
8.1.2 Controle de mudanças operacionais
8.1.3 Procedimentos para o gerenciamento de incidentes
8.1.4 Segregação de funções
8.1.5 Separação dos ambientes de desenvolvimento e de produção
8.1.6 Gestão de recursos terceirizados
8.2 Planejamento e aceitação dos sistemas
8.2.1 Planejamento de capacidade
8.2.2 Aceitação de sistemas
8.3 Proteção contra software malicioso
8.3.1 Controles contra software malicioso
8.4 Housekeeping
8.4.1 Cópias de segurança
8.4.2 Registros de operação
8.4.3 Registro de falhas
8.5 Gerenciamento de rede
8.5.1 Controles da rede
8.6 Segurança e tratamento de mídias
8.6.1 Gerenciamento de mídias removíveis
8.6.2 Descarte de mídias
8.6.3 Procedimentos para tratamento de informação
8.6.4 Segurança da documentação dos sistemas
8.7 Troca de informações e software
8.7.1 Acordos para a troca de informações e software
8.7.2 Segurança de mídias em trânsito
8.7.3 Segurança do comércio eletrônico
8.7.4 Segurança do correio eletrônico
8.7.4.1 Riscos de segurança
8.7.4.2 Política de uso do correio eletrônico
8.7.5 Segurança dos sistemas eletrônicos de escritório
8.7.6 Sistemas disponíveis publicamente
8.7.7 Outras formas de troca de informação


9. Controle de acesso
9.1 Requisitos do negócio para controle de acesso
9.1.1 Política de controle de acesso
9.1.1.1 Requisitos do negócio e política
9.1.1.2 Regras de controle de acesso
9.2 Gerenciamento de acessos do usuário
9.2.1 Registro de usuário
9.2.2 Gerenciamento de privilégios
9.2.3 Gerenciamento de senha dos usuários
9.2.4 Análise crítica dos direitos de acesso do usuário
9.3 Responsabilidades do usuário
9.3.1 Uso de senhas
9.3.2 Equipamentos de usuário sem monitoração
9.4 Controle de acesso à rede
9.4.1 Política de utilização dos serviços da rede
9.4.2 Rota de rede obrigatória
9.4.3 Autenticação para conexão externa do usuário
9.4.4 Autenticação de nó
9.4.5 Proteção de portas de diagnóstico remotas
9.4.6 Segregação de redes
9.4.7 Controle de conexões de rede
9.4.8 Controle do roteamento de rede
9.4.9 Segurança dos serviços de rede
9.5 Controle de acesso ao sistema operacional
9.5.1 Identificação automática de terminal
9.5.2 Procedimentos de entrada no sistema(log-on)
9.5.3 Identificação e autenticação de usuário
9.5.4 Sistema de gerenciamento de senhas
9.5.5 Uso de programas utilitários
9.5.6 Alarme de intimidação para a salvaguarda de usuários
9.5.7 Desconexão de terminal por inatividade
9.5.8 Limitação do tempo de conexão
9.6 Controle de acesso às aplicações
9.6.1 Restrição de acesso à informação
9.6.2 Isolamento de sistemas sensíveis
9.7 Monitoração do uso e acesso ao sistema
9.7.1 Registro (log) de eventos
9.7.2 Monitoração do uso do sistema
9.7.2.1 Procedimentos e áreas de risco
9.7.2.2 Fatores de risco
9.7.2.3 Registro e análise crítica dos eventos
9.7.3 Sincronização dos relógios
9.8 Comuptação móvel e trabalho remoto
9.8.1 Computação móvel
9.8.2 Trabalho remoto


10. Desenvolvimento e manutenção de sistemas
10.1 Requisitos de segurança de sistemas
10.1.1 Análise e especificação dos requisitos de segurança
10.2 Segurança nos sistemas de aplicação
10.2.1 Validação de dados de entrada
10.2.2 Controle do processamento interno
10.2.2.1 Áreas de risco
10.2.2.2 Checagens e controles
10.2.3 Autenticação de mensagem
10.2.4 Validação dos dados de saída
10.3 Controles de criptografia
10.3.1 Política para o uso de controles de criptografia
10.3.2 Criptografia
10.3.3 Assinatura digital
10.3.4 Serviços de não repúdio
10.3.5 Gerenciamento de chaves
10.3.5.1 Proteção de chaves criptográficas
10.3.5.2 Normas, procedimentos e métodos
10.4 Segurança de arquivos do sistema
10.4.1 Controle de software em produção
10.4.2 Produção de dados de teste do sistema
10.4.3 Controle de acesso a bibliotecas de programa-fonte
10.5 Segurança nos processos de desenvolvimento e suporte
10.5.1 Procedimentos de controle de mudanças
10.5.2 Análise crítica das mudanças técnicas do sistema operacional da produção
10.5.3 Restrições nas mudanças dos pacotes de software
10.5.4 Covert Channels e cavalo de tróia
10.5.5 Desenvolvimento terceirizado de software


11. Gestão da continuidade do negócio
11.1 Aspectos da gestão da continuidade do negócio
11.1.1 Processo de gestão da continuidade do negócio
11.1.2 Continuidade do negócio e análise de impacto
11.1.3 Documentando e implementando planos de continuidade
11.1.4 Estrutura do plano de continuidade do negócio
11.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio
11.1.5.1 Teste dos planos
11.1.5.2 Manutenção e reavaliação dos planos
12. Conformidade
12.1 Conformidade com requisitos legais
12.1.1 Identificação da legislação vigente
12.1.2 Direitos e propriedade intelectual
12.1.2.1 Direitos autorais
12.1.2.2 Direitos autorais de software
12.1.3 Salvaguarda de registros organizacionais
12.1.4 Proteção de dados e privacidade da informação pessoal
12.1.5 Prevenção contra uso indevido de recursos de processamento da informação
12.1.6 Regulamentação de controles de criptografia
12.1.7 Coleta de evidências
12.1.7.1 Regras para evidências
12.1.7.2 Admissibilidade da evidência
12.1.7.3 Qualidade e inteireza da evidência
12.2 Análise crítica da política de segurança e da conformidade técnica
12.2.1 Conformidade com a política de segurança
12.2.2 Verificação da conformidade técnica
12.3 Considerações quanto à auditoria de sistemas
12.3.1 Controles de auditoria de sistema
12.3.2 Proteção das ferramentas de auditoria de sistemas

ANEXO B - Representação Gráfica da abrangência da M.A.S